BOMGAR™

Privileged Access Management
Administratieve gids versie 15.3

TC:5/6/2016

Inhoudsopgave

Administratieve gids voor Bomgar Privileged Access Management

In deze gids staat een gedetailleerd overzicht van **/login**. De gids is bedoeld om u te helpen Bomgar gebruikers en uw Bomgar software te beheren. De Bomgar Box dient als het centrale punt voor administratie en beheer van uw Bomgar software en stelt u in staat om in te loggen van elke plaats met internettoegang om de toegangsconsole te downloaden.

Gebruik deze gids pas nadat een beheerder de eerste instelling en configuratie van de Bomgar Box heeft uitgevoerd zoals beschreven in de Hardware-installatiegids voor Bomgar Boxen. Nadat Bomgar correct is geïnstalleerd, kunt u direct toegang krijgen tot uw eindpunten. Als u assistentie nodig hebt, kunt u contact opnemen met Bomgar technische ondersteuning via help.bomgar.com.

TC: 26 januari 2016

Inloggen op de beheerinterface

Inloggen

Log in op de beheerinterface door naar de URL van uw apparaat te gaan gevolgd door **/login**. Beheerders kunnen met de gebruikersbeheer-interface gebruikersaccounts aanmaken en software-instellingen configureren.

Hoewel de URL van uw apparaat elke geregistreerde DNS kan zijn, is dit zeer waarschijnlijk een subdomein van het primaire domein van uw bedrijf (bijv. access.example.com/login).

Standaard gebruikersnaam: **admin**

Standaard wachtwoord: **password**

Opmerking: *Om beveiligingsredenen zijn de administratieve gebruikersnaam en het wachtwoord voor de /appliance interface anders dan die gebruikt worden voor de /login interface. Beide moeten afzonderlijk worden beheerd.*

Opmerking: *Als meervoudige verificatie voor uw account is ingeschakeld, dan moet u de e-mailcode invoeren die u hebt ontvangen. Als u drie keer achter elkaar de e-mailcode verkeerd invoert, dan moet u uw inloggegevens opnieuw invoeren en een nieuwe e-mailcode krijgen.*

Gebruik geïntegreerde browserverificatie

Als Kerberos juist is geconfigureerd voor eenmalige aanmelding, dan kunt u op de koppeling klikken om geïntegreerde browserverificatie te gebruiken zodat u direct in de web-interface kunt komen zonder uw inloggegevens in te moeten voeren.

Uw wachtwoord vergeten?

Als op de pagina **/login > Beheer > Beveiliging** wachtwoord resetten is ingeschakeld, dan is deze koppeling zichtbaar. Om uw wachtwoord te resetten, moet u op de link klikken, uw gebruikersnaam invoeren en vervolgens de beveiligingsvraag goed beantwoorden. Beheerders kunnen hun wachtwoorden met behulp van de beveiligingsvraag niet opnieuw instellen.

Inlogovereenkomst

Beheerders kunnen de toegang tot het inlogscherm beperken door een vereiste inlogovereenkomst in te schakelen die moet worden bevestigd voordat het inlogscherm wordt weergegeven. U kunt de inlogovereenkomst inschakelen en aanpassen op de pagina **/login > Beheer > Websiteconfiguratie**.

Status

Informatie: Gegevens over software voor Bomgar Privileged Access Management bekijken

Sitestatus

De hoofdpagina van de Bomgar /login interface voor Privileged Access Management bevat een overzicht van de statistieken voor uw Bomgar Box. Als u contact opneemt met Bomgar technische ondersteuning voor software-updates of voor het oplossen van problemen, dan kan u worden gevraagd per e-mail een schermopname van deze pagina te verzenden.

Tijdzone

Een beheerder kan uit een vervolgkeuzemenu de juiste tijdzone selecteren door de juiste datum en tijd van het apparaat in te stellen voor de geselecteerde regio.

Totaal aantal toegestane Jump-clients

Bekijk het totale aantal actieve en passieve Jump-clients die op uw systeem zijn toegestaan. Dit aantal wordt bepaald door de hardware-capaciteit van uw Bomgar Box.

Maximale aantal gelijktijdige gebruikers

Bekijk het maximale aantal gebruikers die tegelijkertijd op de toegangsconsole kunnen zijn ingelogd. Dit aantal wordt bepaald door de hardware-capaciteit van uw Bomgar Box.

Eindpunt-licenties

Bekijk het aantal eindpuntlicenties dat op uw Bomgar Box beschikbaar is. Eindpunten zijn Jump-clients, snelkoppelingen naar externe Jumps, snelkoppelingen naar lokale Jumps, snelkoppelingen voor bureaublad op afstand en snelkoppelingen naar Shell Jumps. Neem contact op met Bomgar Sales als u meer licenties nodig hebt.

Geconfigureerde eindpunten

Bekijk het aantal eindpunten dat op uw Bomgar Box is geconfigureerd. Eindpunten zijn Jump-clients, snelkoppelingen naar externe Jumps, snelkoppelingen naar lokale Jumps, snelkoppelingen voor bureaublad op afstand en snelkoppelingen naar Shell Jumps.

Rapport van licentiegebruik downloaden

Download een zip-bestand met gedetailleerde informatie over het gebruik van uw Bomgar licenties. Dit bestand bevat een lijst met alle jumpsnelkoppelingen (exclusief de niet-geïnstalleerde Jump-clients), dagtellingen voor bewerkingen op jumpsnelkoppelingen en licentiegebruik en een samenvatting van de Bomgar Box en het eindpuntlicentiegebruik en het verloop ervan.

Opnieuw starten

U kunt de Bomgar software op afstand opnieuw opstarten. Start uw software opnieuw op als u van Bomgar technische ondersteuning daar opdracht toe krijgt.

De clientsoftware gebruikt als eerste

Dit is de hostnaam waar de Bomgar clientsoftware verbinding mee maakt. Als de hostnaam die door de clientsoftware geprobeerd wordt, moet wijzigen, dan moet u contact opnemen met Bomgar technische ondersteuning zodat die een software-update kunnen samenstellen.

Verbonden clienten

Bekijk het aantal en het type Bomgar softwareclients dat een verbinding met uw Bomgar Box heeft.

Gebruikers: Ingelogde gebruikers bekijken en berichten verzenden

Ingelogde gebruikers

Bekijk een lijst van op de toegangsconsole ingelogde gebruikers samen met de inlogtijd van elk van hen en of zij sessies uitvoeren.

Beëindigen

U kunt de verbinding van een gebruiker met de toegangsconsole beïndigen.

Bericht naar gebruikers sturen

Stuur een bericht naar alle ingelogde gebruikers via een pop-upvenster in de toegangsconsole.

Uitgebreide beschikbaarheid gebruikers

Bekijk gebruikers waarvoor de uitgebreide beschikbaarheid-modus is ingeschakeld.

Uitschakelen

U kunt de uitgebreide beschikbaarheid van een gebruiker uitschakelen.

Mijn account: Wachtwoord en gebruikersnaam wijzigen, toegangsconsole en andere software downloaden

Bomgar toegangsconsole

Kies platform

Kies het besturingssysteem waarop u deze software wilt installeren. Deze vervolgkeuzelijst heeft als standaard het juiste installatieprogramma voor het gedetecteerde besturingssysteem.

Bomgar toegangsconsole downloaden

Start Privileged Web, toegangsconsole op web-basis.

Download het installatieprogramma voor de Bomgar toegangsconsole.

Als een systeembeheerder het console-installatieprogramma op een groot aantal systemen moet implementeren, dan kan hij of zij het Microsoft installatieprogramma in combinatie met een willekeurig beheerdershulpmiddel gebruiken. Op de commandoregel moet u bij het samenstellen van de opdracht om de console met een MSI te installeren naar de map gaan waar de MSI was gedownload en de opdracht invoeren zoals die op de pagina **Mijn account** staat.

U kunt voor uw MSI-installatie optionele parameters meegeven.

- Met **INSTALLDIR=** kunt u elk geldig pad opgeven naar de map waar u de console wilt installeren.
- Voor **RUNATSTARTUP=** kunt u **0** (standaard) of **1** opgeven. Als u 1 invoert, dan wordt de console telkens opgestart als de computer opstart.
- Voor **ALLUSERS=** kunt u **“”** of **1** (standaard) opgeven. Als u **1** invoert, dan wordt de console voor alle gebruikers van de computer geïnstalleerd, anders alleen voor de huidige gebruiker.
- **SHOULDAUTOUPDATE=1** Als u alleen voor de huidige gebruiker installeert, dan kunt u kiezen of de console automatisch moet worden bijgewerkt telkens wanneer de site wordt bijgewerkt door de waarde 1 in te voeren. Bij **0** (standaard) wordt niet automatisch bijgewerkt maar moet de console handmatig opnieuw worden geïnstalleerd als de site wordt bijgewerkt. Als u de console voor alle gebruikers installeert, dan wordt deze niet automatisch bijgewerkt.

Bomgar Virtuele Smartcard

Een gebruiker moet een stuurprogramma voor de Bomgar virtuele smartcard hebben geïnstalleerd om verificatie via een Bomgar virtuele smartcard uit te kunnen voeren. De computer waar toegang toe wordt verkregen, moet actief zijn in opgewaardeerde modus. Ook moet er ofwel het stuurprogramma voor de Bomgar virtuele smartcard voor een eindpunt zijn geïnstalleerd, of er moet toegang toe worden verkregen via de functie 'Jump naar' van de toegangsconsole. Zie het document Smartcards voor verificatie op afstand.

Windows architectuur selecteren

Kies of u het installatieprogramma voor de virtuele smartcard voor het systeem van de Bomgar gebruiker wilt downloaden of voor het eindpuntsysteem.

Installatieprogramma voor Virtuele Smartcard downloaden

Download het hierboven geselecteerde installatieprogramma voor de virtuele smartcard. Met een virtuele smartcard kunt u op een extern systeem worden geverifieerd via een smartcard op uw lokale systeem.

Bomgar Automatische opwaarderingsservice

Windows architectuur selecteren

Kies het besturingssysteem waarop u deze software wilt installeren. Deze vervolgkeuzelijst heeft als standaard het juiste installatieprogramma voor het gedetecteerde besturingssysteem.

Installatieprogramma voor Automatische opwaarderingsservice downloaden

In bijzondere gevallen moet u mogelijk een sessie starten waarbij de client op het eindpunt al opgewaardeerd draait of moet u mogelijk de client op het eindpunt opwaarderen zonder inloggegevens te verstrekken. Om de client op het eindpunt veilig op te waarderen zonder prompt, moet u de **Bomgar Automatische opwaarderingsservice** downloaden en vooraf op het externe Windows systeem installeren waarnaar u opgewaardeerde toegang zonder inloggegevens wilt hebben. U moet de opwaarderingsservice met een account installeren dat beheerdersrechten op de lokale machine heeft.

Als de opwaarderingsservice wordt uitgevoerd, dan voegt het een hash aan het register toe die uniek is voor uw Bomgar site. Als het externe systeem vervolgens via die site een sessie start, dan controleert de opwaarderingsservice of de hash in het register met de hash in de client overeenkomt. Bij overeenkomst probeert de client een automatische opwaardering.

Registerbestand voor automatische opwaarderingservice downloaden

De hash van uw website wijzigt na een update van de Bomgar software. Download het registerbestand met de opwaarderingsservice om de registerhash te wijzigen op systemen waar de opwaarderingsservice al geïnstalleerd is. U moet het registerbestand met de opwaarderingsservice met een account uitvoeren dat beheerdersmachtigingen op de lokale computer heeft.

Modus Uitgebreide beschikbaarheid

Activeren of uitschakelen

Activeer de modus uitgebreide beschikbaarheid of schakel deze uit door op de knop **Activeren of uitschakelen** te klikken. In de modus uitgebreide beschikbaarheid kunt u, als u niet op de console bent ingelogd, e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen.

Uw e-mailinstellingen wijzigen

E-mailadres

Stel het e-mailadres in waarnaar e-mailkennisgevingen moeten worden verzonden, zoals het opnieuw instellen van het wachtwoord of waarschuwingen over uitgebreide beschikbaarheid-modus.

Voorkeurstaal voor e-mail

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Uw wachtwoord wijzigen

Bomgar beveelt aan uw wachtwoord regelmatig te wijzigen.

Gebruikersnaam, huidig wachtwoord, nieuw wachtwoord

Controleer of u bent ingelogd op het account waarvoor u het wachtwoord wilt wijzigen en voer vervolgens uw huidige wachtwoord in. Maak een nieuw wachtwoord voor uw account aan en bevestig dit. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

Uw beveiligingsvraag/antwoord veranderen

Beveiligingsvraag en antwoord

Een gebruiker kan met de beveiligingsvraag en het antwoord erop een vergeten wachtwoord resetten nadat hij of zij het juiste antwoord op de vraag heeft gegeven. Wachtwoorden mogen alleen worden gereset als **Wachtwoord resetten inschakelen** aangevinkt is op de pagina **Beheer > Beveiliging**. Beheerders kunnen hun wachtwoorden met behulp van de beveiligingsvraag niet opnieuw instellen.

Configuratie

Opties: Verbindingsopties beheren, sessies opnemen

Sessieopties

Afgesloten sessies bij Uitloggen of Afsluiten vereisen

Als u **Afgesloten sessies bij Uitloggen of Afsluiten vereisen** aanvinkt, dan kunnen gebruikers van de console niet uitloggen als zij op dat moment nog sessietabbladen open hebben staan.

Verbindingsopties

Time-out voor nieuwe verbinding

Bepaal hoe lang een eindpuntclient waarvan de verbinding is verbroken, moet proberen opnieuw verbinding te krijgen.

Beperk de fysieke toegang tot het eindpunt als de verbinding met het eindpunt wordt verbroken of als de verbinding met alle gebruikers die bij de sessie aanwezig zijn verbroken is

Als de verbinding met de sessie verloren is gegaan, dan kan de invoer van de muis en het toetsenbord op het externe systeem tijdelijk uitgeschakeld zijn. Beide komen weer beschikbaar als de verbinding is hersteld of als de sessie wordt beëindigd.

Gedrag voor Beëindigen van sessie

U kunt kiezen wat er moet worden gedaan als u binnen de in **Time-out voor nieuwe verbinding** ingestelde periode niet opnieuw verbinding kunt krijgen. Om ervoor te zorgen dat de eindgebruiker niet-geautoriseerde rechten krijgt na een opgewaardeerde sessie, moet u de client zo instellen dat bij het beëindigen van een sessie met een externe Windows computer de eindgebruiker automatisch wordt uitgelogd, de externe computer op slot gaat of dat er niets gebeurt. Deze regels gelden niet voor sessies waarin de browser wordt gedeeld.

Hiermee kunnen gebruikers deze instelling per sessie overschrijven

U kunt tijdens een sessie vanaf het tabblad **Samenvatting** in de console een gebruiker toestaan de instelling voor het afsluiten van de sessie te overschrijven.

Inlogopties voor toegangssessies

Opnames van scherm delen/opdrachtshell inschakelen

Kies of sessies met scherm delen en/of sessies met opdrachtshell automatisch als video's moeten worden opgenomen. Als u opnames van sessies met opdrachtshell inschakelt, komen ook sessies met opdrachtshell als tekst beschikbaar.

Resolutie van de opnames van scherm delen/opdrachtshell

Stel de resolutie in waarmee u het terugspelen van de sessie wilt bekijken.

Opmerking: *Alle opnames worden in ruwe opmaak opgeslagen, de resolutie heeft alleen gevolgen voor het afspelen.*

Automatische registratie van systeeminformatie activeren

Kies of systeeminformatie automatisch aan het begin van de sessie van het externe systeem moet worden opgehaald zodat deze informatie later in de rapporten over de sessie beschikbaar is.

Forensische gegevens van sessies inschakelen

Kies of u de extra mogelijkheid wilt om over alle sessies heen te zoeken op basis van sessie-gebeurtenissen. Dit omvat chatberichten, bestandsoverdracht, gebeurtenissen in de register-editor en gebeurtenissen waardoor het voorgrond-venster van de sessie wijzigt. Deze functie is standaard ingeschakeld.

Opmerking*: Als opdrachtshell is ingeschakeld, dan kunt u met Forensische gegevens van sessies uitgebreid in shell-opnames zoeken. Als u op een zoekterm zoekt en deze wordt gevonden in een opgeslagen shell-opname, dan wordt de video automatisch op dat tijdstip in de opname gepositioneerd. Er worden geen uitvoer van opdrachten en geen wachtwoorden opgenomen.*

Teams: Gebruikers in teams groeperen

Teams :: Beheren

Door gebruikers in teams te groeperen, werkt u efficiënter door leiderschap binnen gebruikersgroepen aan te wijzen. In de toegangsconsole verschijnt elk team als een aparte wachtrij voor sessies.

Nieuw team toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object. Als een team wordt verwijderd, worden de bijbehorende gebruikersaccounts niet verwijderd, alleen het team waartoe zij behoren wordt verwijderd.

Teams :: Toevoegen of bewerken

Algemene instellingen

Teamnaam

Maak een unieke naam aan om te helpen dit object te identificeren.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, wordt er automatisch een aangemaakt.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Groepsbeleidslijnen

Let op eventuele groepsbeleidslijnen waardoor leden aan dit team worden toegewezen. Klik op de koppeling om naar de pagina **Groepsbeleidslijnen** te gaan om beleidsleden te verifiëren of toe te wijzen.

Teamleden

Selecteer uit de lijst met beschikbare gebruikers een of meer gebruikers en klik op het pijltje om ze in het team te zetten.

U kunt de rol van elk van de leden instellen op **Teamlid**, **Teamleider** of **Teammanager**. Deze rollen zijn van groot belang in de **Dashboard**-functie van de toegangsconsole.

Teamleden die het lidmaatschap delen via een of meer groepsbeleidslijnen staan in de lijst samen met een koppeling naar de configuratiepagina **Groepsbeleidslijnen**.

Toegang tot een Jump-client

Toestemming voor toegang gegeven door dit team

Selecteer welke teams toegang moeten hebben tot Jump-clients die aan de Jumpgroep van dit team zijn vastgespeld. Standaard heeft alleen dit team toegang tot zijn eigen Jump-clients. Maar u kunt meerdere andere teams selecteren om de Jump-clients van dit team te zien en een Jump ernaar uit te voeren.

Toestemming voor toegang gegeven aan dit team

Bekijk een lijst met andere teams die de toegang tot Jump-clients met leden van dit team delen.

Teams :: Dashboard-instellingen

Een gebruiker kan binnen een team alleen andere gebruikers beheren die een lagere rol hebben dan hij of zij zelf heeft. Let er echter op dat rollen strikt binnen een bepaald team gelden, zodat een gebruiker in het ene team een andere gebruiker kan beheren, maar diezelfde gebruiker in een ander team niet kan beheren.

Teamleden vanaf Dashboard controleren

Als dit is ingeschakeld, dan kan een teamleider vanaf het dashboard met teamleden meekijken. Kies een selectie voor het **Uitschakelen** van de mogelijkheid tot meekijken of kies **Alleen toegangsconsole** om een teamleider of beheerder op de toegangsconsole van een teamlid mee te laten kijken. Meekijken is van toepassing op alle teamleiders en beheerders voor alle teams op de site.

Sessie verplaatsen en Overnemen in dashboard activeren

Als deze optie is aangevinkt, dan kan een teamleider de sessies van een teamlid overnemen of overdragen. Ook kan een teammanager zowel teamleden als teamleiders beheren.

Jump

Jump-clients: Instellingen van Jump-clients voor toegang tot eindpunten beheren en installeren

Wizard voor massa-implementatie van Jump-clients

Beheerders en bevoorrechte gebruikers kunnen de wizard voor massa-implementatie gebruiken om Jump-clients op een of meer externe computers te installeren om later toegang zonder toezicht tot deze computers te krijgen.

Overschrijven tijdens installatie toestaan

Bepaalde instellingen voor de wizard voor massa-implementatie kunnen worden overschreven, zodat u de opdrachtregel kunt gebruiken om vóór de installatie parameters in te stellen die specifiek zijn voor uw implementatie.

Jumpgroep

Selecteer uit de vervolgkeuzelijst of de Jump-client aan uw persoonlijke Jumpgroep moet worden vastgespeld of aan een Jumpgroep van een team. Als de Jump-client aan uw persoonlijke Jumpgroep is vastgespeld, dan bent u de enige die via deze Jump-client toegang tot deze externe computer kan krijgen. Als de Jump-client aan een Jumpgroep van een team is vastgespeld, dan is deze Jump-client beschikbaar voor alle leden van teams die toegang tot de Jump-clients van dit team hebben.

Jump-beleid

U kunt op deze Jump-client een **Jump-beleid** toepassen. Jump-beleidslijnen worden op de pagina **Jump > Jump-beleidslijnen** geconfigureerd en bepalen gedurende welke periodes een gebruiker toegang tot deze Jump-client kan krijgen. Er kan ook een kennisgeving worden verzonden als het Jump-beleid wordt benaderd of er kan toestemming moeten worden gevraagd om het te benaderen. Als er geen Jump-beleid is toegepast, dan kan zonder beperking toegang tot deze Jump-client worden verkregen.

Tag

Door een **tag** toe te voegen, kunt u uw Jump-clients binnen de toegangsconsole in categorieën organiseren.

Type verbinding

Stel het **Type verbinding** in op **Actief** of **Passief** voor de Jump-clients die worden geïmplementeerd.

Proxy voor Jumpoint

Als u een of meer Jumpoints als proxy hebt ingesteld, dan kunt u een Jumpoint selecteren om als proxy op te treden voor verbindingen naar deze Jump-clients. Op die manier kunnen deze Jump-clients, als zij op computers zonder eigen internetverbinding zijn geïnstalleerd, het Jumpoint gebruiken om een verbinding terug naar uw Bomgar Box te maken. De Jump-clients moeten op hetzelfde netwerk zijn geïnstalleerd als het Jumpoint dat geselecteerd is om voor de verbindingen als proxy op te treden.

Opmerkingen

Voeg **Opmerkingen** toe die handig kunnen zijn bij het zoeken naar en identificeren van externe computers. Bedenk dat alle Jump-clients die via dit installatieprogramma zijn geïmplementeerd in eerste instantie dezelfde opmerkingen hebben, tenzij u **Overschrijven toestaan tijdens installatie** aanvinkt en de individuele parameters gebruikt om het installatieprogramma voor individuele programma's aan te passen.

Dit installatieprogramma is geldig gedurende

Het installatieprogramma blijft te gebruiken gedurende de periode die gespecificeerd is in de vervolgkeuzelijst **Dit installatieprogramma is geldig gedurende**. Zorg dat u voldoende tijd reserveert voor het installeren. Als iemand zou proberen na deze periode het installatieprogramma voor de Jump-client uit te voeren, dan mislukt de installatie en moet een nieuw installatieprogramma voor de Jump-client worden aangemaakt. Deze periode kan op een willekeurige waarde van 10 minuten tot 1 jaar worden ingesteld. Deze periode heeft GEEN invloed op hoe lang de Jump-client actief blijft.

Probeer een opgewaardeerde installatie als de client dit ondersteunt

Als **Probeer een opgewaardeerde installatie als de client dit ondersteunt** is geselecteerd, dan probeert het installatieprogramma met beheerdersrechten te starten om de Jump-client als een systeemservice te installeren. Als de poging tot een opgewaardeerde installatie niet slaagt of als deze optie niet is geselecteerd, dan start het installatieprogramma met gebruikersrechten en wordt de Jump-client als een toepassing geïnstalleerd. Deze opties is alleen van toepassing op Windows en Mac besturingssystemen.

> ***Opmerking:*** *Een Jump-client die in gebruikersmodus is vastgespeld is alleen beschikbaar als die gebruiker ingelogd is. Daar staat tegenover dat een Jump-client die in servicemodus is vastgespeld, met opgewaardeerde rechten, toestaat dat het systeem altijd beschikbaar is, ongeacht of de gebruiker ingelogd is of niet.*

Prompt voor inloggegevens voor opwaardering indien nodig

Als **Prompt voor inloggegevens voor opwaardering, indien nodig** is geselecteerd, dan vraagt het installatieprogramma de gebruiker om beheerders-inloggegevens in te voeren als het systeem vereist dat deze inloggegevens onafhankelijk worden ingevoerd, anders wordt de Jump-client met gebruikersrechten geïnstalleerd. Dit is alleen van toepassing als de gebruiker een opgewaardeerde installatie probeert uit te voeren.

Eindpunt-client geminimaliseerd starten wanneer de sessie gestart wordt

Door **Eindpunt-client geminimaliseerd starten wanneer de sessie gestart wordt** te selecteren wordt de eindpunt-client niet actief en blijft deze geminimaliseerd in de taakbalk of gedokt staan als een sessie door een van deze Jump-clients wordt gestart.

Hulp bij massa-implementatie

Systeembeheerders die het installatieprogramma voor de Jump-client op een groot aantal systeem moeten implementeren kunnen het uitvoerbare Windows MSI installatieprogramma voor Windows, Mac of Linux gebruiken samen met een willekeurig beheerderhulpmiddel. U kunt een geldig pad opgeven naar de map waar u de Jump-client wilt installeren. U kunt, al naar gelang uw wensen, bepaalde installatieparameters ook overschrijven. Deze parameters kunnen zowel voor de MSI als voor de EXE worden gespecificeerd met een hulpmiddel voor systeembeheer of met de interface met opdrachtregel. Als u bepaalde installatie-opties markeert om tijdens installatie te worden overschreven, dan kunt u de volgende parameters gebruiken om het installatieprogramma voor de Jump-client voor individuele installaties aan te passen. Denk eraan dat als u een parameter op de opdrachtregel ingeeft, maar deze in de /login beheerinterface niet is gemarkeerd voor overschrijven, dat de installatie dan mislukt. Als de installatie mislukt, kunt u in het gebeurtenislogboek van het besturingssysteem de installatiefouten bekijken.

Opdrachtregel-parameter	Waarde	Beschrijving
--install-dir	<directory_path>	Hier specificeert u een nieuwe schrijfbare map waaronder u de Jump-client wilt installeren. Dit wordt alleen op Windows en Linux ondersteund. Als u een aangepaste map voor installatie wilt definiëren, dan moet u controleren of de map die u wilt aanmaken niet al bestaat en op een locatie is waar u mag schrijven.
--jc-jump-group	gebruiker: <gebruikersnaam> team:<team-code-naam>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter de in de Wizard voor massa-implementatie gespecificeerde Jumpgroep overschreven.
--jc-session-policy	<session-policy-code-name>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter het sessiebeleid ingesteld dat het machtigingsbeleid tijdens een toegangssessie bepaalt.
--jc-jump-policy	<jump-policy-code-name>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter het Jump-beleid ingesteld dat regelt hoe gebruikers een Jump naar de Jump-client kunnen uitvoeren.
--jc-tag	<tag-naam>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter de tag van de Jump-client ingesteld.
--jc-comments	<opmerkingen ... >	Als overschrijven is toegestaan, dan worden met deze opdrachtregel-parameter de opmerkingen van de Jump-client ingesteld.

Opmerking: *Als een MSI-installatieprogramma geïmplementeerd wordt in Windows met gebruik van de msiexec-opdracht, dan kunnen de bovenstaande parameters worden gespecificeerd door:*

1. *Voorafgaande streepjes (-) te verwijderen*
2. *Overgebleven streepjes naar onderstrepingstekens (_) te converteren*
3. *Met een gelijkteken (=) een waarde toe te kennen*

Voorbeeld:

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

De enige uitzondering op deze regel is ***installdir****, die in de EXE-versie een streepje bevat maar in de MSI-versie niet.*

Client nu downloaden of installeren

Platform

Kies het besturingssysteem waarop u deze software wilt installeren. Deze vervolgkeuzelijst heeft als standaard het juiste installatieprogramma voor het gedetecteerde besturingssysteem.

NB: in tegenstelling tot de toegangsconsole worden Jump-clients die vanuit een MSI-bestand zijn geïnstalleerd, niet automatisch bijgewerkt.

Downloaden/installeren

U kunt het installatieprogramma direct downloaden als u van plan bent om het met een hulpmiddel voor systeembeheer te distribueren of als u bij de computer bent waartoe u later toegang wilt krijgen.

Implementatie naar e-mailgeadresseerden

E-mail

U kunt het installatieprogramma ook naar een of meerdere externe gebruikers e-mailen. Meerdere ontvangers kunnen de client met dezelfde koppeling installeren.

Statistieken voor Jump-Clients

Een beheerder kan kiezen welke statistieken voor alle Jump-clients hij of zij bekijkt voor een gehele site. Deze statistieken worden in de toegangsconsole weergegeven en bevatten besturingssysteem, bedrijfstijd, console-gebruiker, CPU, schijfgebruik en een miniatuurweergave van het externe scherm. Bestaande Jump-clients laten de wijzigingen in de Jump-clientstatistieken zien wanneer deze de volgende keer worden bijgewerkt.

Instellingen voor Jump-Clients

Interval voor bijwerken statistieken van actieve Jump-clients

Interval voor bijwerken statistieken van actieve Jump-clients bepaalt hoe vaak deze statistieken worden bijgewerkt. Door te beheren welke statistieken hoe vaak bekeken worden kan de hoeveelheid gebruikte brandbreedte worden beperkt. Hoe meer actieve Jump-clients u hebt geïmplementeerd, hoe minder statistieken u wilt genereren en hoe langer u het interval in wilt stellen.

Maximaal aantal gelijktijdige upgrades van Jump-clients

Stel ook het maximale aantal Jump-clients in dat tegelijkertijd mag worden bijgewerkt. Bedenk dat als u een groot aantal Jump-clients geïmplementeerd hebt, u dit aantal mogelijk moet beperken om de hoeveelheid gebruikte bandbreedte te regelen.

> ***Opmerking**: Deze instelling heeft geen invloed op het bijwerken van de toegangsconsole.*

Maximale bandbreedte voor gelijktijdige upgrades van Jump-clients

U kunt de tijdens het bijwerken gebruikte bandbreedte verder regelen door de instelling **Maximale bandbreedte voor gelijktijdige upgrades van Jump-clients**.

> ***Opmerking**: Deze instelling heeft geen invloed op het bijwerken van de toegangsconsole.*

Gelijktijdige toegang door gebruikers tot één enkele Jump-client toestaan

De optie **Gelijktijdige toegang door gebruikers tot één enkele Jump-client toestaan** biedt een mogelijkheid voor meerdere gebruikers om toegang tot dezelfde Jump-client te krijgen zonder dat zij door een andere gebruiker moeten worden uitgenodigd om aan een actieve sessie deel te nemen. De eerste gebruiker die tot de Jump-client toegang krijgt, blijft eigenaar van de sessie. Gebruikers in een gedeelde Jump-sessie kunnen elkaar zien en met elkaar chatten.

Opmerking: *Met deze instelling (alleen geïmplementeerd in Windows) kan worden voorkomen dat een klant een Jump-client op zijn of haar lokale machine via een klik op de rechtermuisknop uit het contextmenu in het systeemvak verwijdert. Om de Jump-client te verwijderen kunnen gebruikers met de juiste rechten op de clientmachine dit doen met de standaard Windows-functie Software toevoegen/verwijderen. Als deze instelling wordt gewijzigd, wordt deze opnieuw op een Jump-client toegepast wanneer er een nieuwe verbinding met het apparaat wordt gemaakt.*

Gebruikers toestaan om te proberen Jump-clients uit de slaapstand te halen

Gebruikers toestaan om te proberen Jump-clients uit de slaapstand te halen biedt de mogelijkheid om een geselecteerde Jump-client uit slaapmodus te halen door Wake-on-LAN (WOL) pakketten via een andere Jump-client op hetzelfde netwerk te sturen. Als een poging tot WOL is uitgevoerd, dan is deze optie gedurende 30 seconden niet beschikbaar. Pas daarna kan een volgende poging worden ondernomen. WOL moet op de doelcomputer en het netwerk zijn ingeschakeld om deze functie te kunnen gebruiken. De standaard gateway-informatie van de Jump-client wordt gebruikt om te bepalen of andere Jump-clients zich op hetzelfde netwerk bevinden. Bij het verzenden van een WOL-pakket heeft de gebruiker een geavanceerde optie om een wachtwoord mee te geven voor WOL-omgevingen waar zo'n WOL-wachtwoord vereist is.

Standaard verbindingstype voor Jump-client

Stel in of het standaard type Jump-client-verbinding actief of passief moet zijn.

Poort voor passieve Jump-client

Met **Poort voor passieve Jump-client** kunt u specificeren welke poort een passieve Jump-client gebruikt om naar een opdracht “uit slaapmodus halen” van het apparaat te luisteren. De standaard poort is 5832. Controleer of de instellingen van de firewall inkomend verkeer via deze poort toestaan voor uw hosts met passieve Jump-clients. Nadat een Jump-client actief is geworden, maakt deze altijd een verbinding met het apparaat via poort 80 of 443 uitgaand.

Jump-beleidslijnen: Roosters, kennisgevingen en toestemmingen voor jumpsnelkoppelingen instellen

Jump-beleidslijnen

Nieuwe Jump-beleidslijn toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Jump-beleidslijnen :: Toevoegen

Schermnaam

Maak een unieke naam aan om te helpen dit object te identificeren. Deze naam moet de gebruikers helpen dit beleid te identificeren als het aan Jump-clients wordt toegekend.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, wordt er automatisch een aangemaakt.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit object samen te vatten.

Jump-rooster: Ingeschakeld

Stel een rooster in om te definiëren wanneer onder dit beleid toegang tot Jump-clients kan worden verkregen. Stel de tijdzone in die u voor dit rooster wilt gebruiker en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als bijvoorbeeld de begintijd is ingesteld op 08:00 uur en de eindtijd op 17:00 uur, dan kan een gebruiker een sessie met deze Jump-client op elk tijdstip in deze periode starten en kan blijven doorwerken tot na de eindtijd. De gebruiker kan echter na 17:00 uur niet opnieuw toegang tot de sessie krijgen.

Forceer beëindiging van sessie als het rooster toegang niet toestaat

Als strikter toegangsbeheer noodzakelijk is, moet u het veld **Beëindiging van sessie forceren** aanvinken. Hierdoor wordt geforceerd dat op het geplande tijdstip de verbinding met de sessie wordt verbroken. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd.

Jump-mededeling: Geadresseerden berichten wanneer een sessie start

Als deze optie is aangevinkt, dan wordt een kennisgeving per e-mail naar de aangegeven ontvangers verzonden wanneer een sessie met een Jump-client wordt gestart die dit Jump-beleid gebruikt. Als een gebruiker probeert een sessie te starten met een

Jump-client die dit beleid gebruikt, dan verschijnt een prompt dat een e-mailmelding wordt verzonden waarin wordt gevraagd of de gebruiker de sessie toch wil starten.

Geadresseerden berichten wanneer een sessie stopt

Als deze optie is aangevinkt, dan wordt een kennisgeving per e-mail naar de aangegeven ontvangers verzonden wanneer een sessie met een Jump-client beëindigt die dit Jump-beleid gebruikt. Als een gebruiker probeert een sessie te starten met een Jump-client die dit beleid gebruikt, dan krijgt hij of zij een prompt waarin staat dat aan het eind van de sessie een e-mailmelding wordt verzonden en waarin wordt gevraagd of de gebruiker de sessie toch wil starten.

E-mailadres(sen)

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden. Voor deze functie is een geldige SMTP-configuratie voor uw apparaat vereist. U kunt deze instellen op de pagina **/login > Beheer > E-mailconfiguratie**.

Schermnaam

Voer de naam van de e-mailgeadresseerde in. Deze naam verschijnt bij de prompt die de gebruiker ziet vóór een sessie met een Jump-client die deze beleidslijn gebruikt.

Regio

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Jump-goedkeuring: Ticket-ID vereist voordat een sessie start

Als deze optie is aangevinkt, dan moet de gebruiker een geldig ticket-ID invoeren voordat een toegangssessie kan starten. Als een gebruiker probeert toegang tot een eindpunt te krijgen wanneer dit Jump-beleid van toepassing is, dan moet de gebruiker een ticket-ID van uw bestaande ITSM of goedkeuringsproces voor een ticket-ID invoeren voordat toegang wordt verleend. Configureer de integratie met de ITSM of het ticketsysteem vanuit de sectie **Jump-beleidslijnen :: Ticketsysteem**.

Toestemming vereisen voordat een sessie start

Als deze optie is aangevinkt, dan wordt een kennisgeving per e-mail naar de aangegeven ontvangers verzonden wanneer gepoogd wordt een sessie met een Jump-client te starten die dit Jump-beleid gebruikt. Als een gebruiker probeert een sessie te starten met een jumpsnelkoppeling die dit beleid gebruikt, dan verschijnt een dialoog waarin de gebruiker wordt gevraagd een reden voor het verzoek in te voeren evenals het tijdstip en de duur van het verzoek.

Maximale toegangsduur

Stel de maximale tijdsduur in waarvoor een gebruiker toegang kan aanvragen tot een Jump-client die dit beleid gebruikt. De gebruiker kan een kortere tijdsduur aanvragen, maar geen langere dan hier is ingesteld.

E-mailadres(sen)

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden. Voor deze functie is een geldige SMTP-configuratie voor uw apparaat vereist. U kunt deze instellen op de pagina **/login > Beheer > E-mailconfiguratie**.

Schermnaam

Voer de naam van de e-mailgeadresseerde in. Deze naam verschijnt bij de prompt die de gebruiker ziet vóór een sessie met een Jump-client die deze beleidslijn gebruikt.

Regio

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Jump-beleidslijnen :: Sjabloon voor kennisgeving per e-mail

Onderwerp

Pas het onderwerp van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Body

Pas de inhoud van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Jump-beleidslijnen :: Sjabloon voor goedkeuring per e-mail

Onderwerp

Pas het onderwerp van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Body

Pas de inhoud van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Jump-beleidslijnen :: Ticketsysteem

URL van ticketsysteem

Voer in **URL van ticketsysteem** de URL in voor uw externe ticketsysteem. De Bomgar Box verzendt een uitgaand verzoek naar uw externe ticketsysteem. De URL moet de juiste opmaak hebben voor HTTP of HTTPS. Als u een HTTPS-URL invoert, dan moet het certificaat van de site geverifieerd zijn om een geldige verbinding te maken. Als er een Jumpbeleid bestaat waarvoor een ticket-ID vereist is, dan moet een URL voor het ticketsysteem zijn ingevoerd, anders ontvangt u een waarschuwing.

Huidige status

Het veld **Huidige status** wordt alleen getoond als er een geldige statuswaarde bestaat om de verbinding te rapporteren met het ticketsysteem dat in **URL van ticketsysteem** geconfigureerd is. Bij elke wijziging in de configuratie van het ticketsysteem wordt de

waarde opnieuw ingesteld.

Een certificaat voor een HTTPS-verbinding uploaden

Klik op **Bestand kiezen** om het certificaat voor de verbinding van het HTTPS-ticketsysteem naar het apparaat te uploaden. Als het certificaat is geüpload, dan gebruikt het apparaat dit wanneer het met het externe systeem contact maakt. Als u geen certificaat uploadt en onderstaand keuzevakje **SSL-certificaatfouten negeren** is aangevinkt, dan kan de Bomgar Box als optie terugvallen op het ingebouwde certificaatarchief wanneer het verzoek wordt verzonden.

SSL-certificaatfouten negeren

Als deze optie is aangevinkt, dan neemt de Bomgar Box **niet** de informatie om het certificaat te valideren op als het met het externe ticketsysteem contact maakt. Zorg dat deze optie niet is aangevinkt als u een certificaat voor een beveiligde HTTPS-verbinding uploadt.

Gebruikersprompt

Voer in **Gebruikersprompt** de tekst voor de dialoog in die u wilt dat gebruikers van toegangsconsole zien als hun gevraagd wordt om een voor toegang vereiste ticket-id in te voeren.

Jumpoint: Toegang zonder toezicht naar een netwerk instellen

Jumpoint beheer

Met de Jump-technologie van Bomgar kan een gebruiker toegang krijgen tot computers op een extern netwerk zonder vooraf op elke machine software te moeten installeren. Er hoeft alleen een enkele Jumpoint-agent op een willekeurige netwerklocatie te zijn geïnstalleerd om zonder toezicht toegang tot elke pc in dat netwerk te krijgen.

Nieuw Jumpoint toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Opnieuw implementeren

Verwijder de installatie van een Jumpoint en download een installatieprogramma om het bestaande Jumpoint door een nieuw te vervangen. Snelkoppelingen voor een Jump met het bestaande Jumpoint zullen het nieuwe Jumpoint gebruiken als dat geïnstalleerd is.

Opmerking: *Als een bestaand Jumpoint wordt vervangen, dan wordt de configuratie ervan niet opgeslagen. Het nieuwe Jumpoint moet opnieuw worden geconfigureerd.*

Jumpoint :: Toevoegen of bewerken

Naam

Maak een unieke naam aan om te helpen dit object te identificeren. Deze naam helpt gebruikers om dit Jumpoint te lokaliseren als zij een sessie met een computer op hetzelfde netwerk moeten opstarten.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, wordt er automatisch een aangemaakt.

Uitgeschakeld

Als dit is aangevinkt, dan kan het Jumpoint geen Jump-verbindingen maken.

Geclusterd

Als dit is aangevinkt, dan kunt u meerdere, redundante nodes van hetzelfde Jumpoint op verschillende hostsystemen toevoegen. Zo zorgt u ervoor dat het Jumpoint beschikbaar blijft zolang er tenminste één node online blijft.

Shell Jump activeren

Als u gebruikers wilt toestaan om via dit Jumpoint verbinding te maken met netwerkapparaten met SSH of Telnet, moet u **Toegang tot Shell Jump activeren** aanvinken.

Gebruikers toevoegen

Vanaf de pagina Jumpoint bewerken kunt u gebruikers autoriseren om via dit Jumpoint sessies te starten. Nadat een Jumpoint is aangemaakt kunt u ook vanuit **Gebruikers en beveiliging > Groepsbeleidslijnen** toegang toekennen aan groepen gebruikers .

Wizard voor bulkimport van snelkoppelingen naar Jumps

Als u een groot aantal snelkoppelingen naar Jumps aanmaakt, dan is het misschien eenvoudiger om deze uit een spreadsheet te importeren dan om ze een voor een in de toegangsconsole toe te voegen. Selecteer uit het vervolgkeuzemenu **Wizard voor bulkimport van snelkoppelingen naar Jumps** het type Jumpsnelkoppeling dat u wilt toevoegen en klik vervolgens op **Sjabloon downloaden**. Gebruik de tekst uit de CSV-sjabloon als kolomkoppen en voeg de informatie toe voor elke snelkoppeling naar een Jump die u wilt importeren. Optionele velden kunnen worden ingevuld of leeg blijven.

Nadat u de sjabloon helemaal hebt ingevuld, kunt u **Snelkoppelingen naar Jumps importeren** gebruiken om het CSV-bestand met de informatie over de jumpsnelkoppelingen te uploaden. Elk CSV-bestand kan maar één type jumpsnelkoppeling bevatten. De opmaak van het CSV-bestand moet aan onderstaande tabellen voldoen. De maximale bestandsgrootte die in één keer kan worden geüpload is 5 MB.

Lokale jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt waarop toegang kan worden verkregen via deze jumpsnelkoppeling.
Jumpgroep	De codenaam van het team waarmee deze jumpsnelkoppeling moet worden geassocieerd. ***Opmerking:*** *Bij gebruik van de importmethode kan een jumpsnelkoppeling niet met een persoonlijke Jumpgroep worden geassocieerd.*
Tag (optioneel)	U kunt uw jumpsnelkoppelingen in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw jumpsnelkoppelingen toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot deze jumpsnelkoppeling te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op deze jumpsnelkoppeling beschikbaar zijn.

Externe jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt waarop toegang kan worden verkregen via deze jumpsnelkoppeling.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Jumpgroep	De codenaam van het team waarmee deze jumpsnelkoppeling moet worden geassocieerd. ***Opmerking:*** *Bij gebruik van de importmethode kan een jumpsnelkoppeling niet met een persoonlijke Jumpgroep worden geassocieerd.*
Tag (optioneel)	U kunt uw jumpsnelkoppelingen in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw jumpsnelkoppelingen toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot deze jumpsnelkoppeling te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op deze jumpsnelkoppeling beschikbaar zijn.

Snelkoppeling naar protocol voor bureaublad op afstand

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt waarop toegang kan worden verkregen via deze jumpsnelkoppeling.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Gebruikersnaam (optioneel)	De gebruikersnaam om u mee aan te melden.
Domein (optioneel)	Het domein waarin het eindpunt zich bevindt.
Weergavegrootte (optioneel)	De resolutie waarmee u het externe systeem wilt bekijken. Dit kan **primair** zijn (de grootte van uw primaire beeldscherm), **alles** (de grootte van al uw beeldschermen bij elkaar) of **XxY** (waar **X** en **Y** een ondersteunde combinatie zijn van breedte en hoogte, bijv. **640x480**).
Kwaliteit (optioneel)	De kwaliteit waarmee u het externe systeem wilt bekijken. Dit kan **low** zijn (zwart-wit voor het laagste gebruik van bandbreedte), **best_perf** (standaard, 8 bit kleur voor snelle prestaties), **perf_and_qual** (16 bit voor gemiddelde kwaliteit en prestaties), of **best_qual** (32 bit voor de hoogste beeldresolutie). Dit kan tijdens de sessie met bureaublad op afstand (RPD) niet worden gewijzigd.
Consolesessie (optioneel)	**1**: Hiermee start een consolesessie. **0**: Hiermee start een nieuwe sessie (standaard).
Onbetrouwbaar certificaat negeren (optioneel)	**1**: Negeert certificaatwaarschuwingen. **0**: Toont een waarschuwing als het certificaat van de server niet kan worden geverifieerd.

Veld	Beschrijving
Jumpgroep	De codenaam van het team waarmee deze jumpsnelkoppeling moet worden geassocieerd. ***Opmerking:*** *Bij gebruik van de importmethode kan een jumpsnelkoppeling niet met een persoonlijke Jumpgroep worden geassocieerd.*
Tag (optioneel)	U kunt uw jumpsnelkoppelingen in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw jumpsnelkoppelingen toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot deze jumpsnelkoppeling te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op deze jumpsnelkoppeling beschikbaar zijn.

Shell Jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt waarop toegang kan worden verkregen via deze jumpsnelkoppeling.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Gebruikersnaam (optioneel)	De gebruikersnaam om u mee aan te melden.
Protocol	Mag **SSH** of **Telnet** zijn.
Poort (optioneel)	Een geldig poortnummer van **1** tot **65535**. Het standaard poortnummer is **22** als het protocol **ssh** is, of **23** als het protocol **telnet** is.
Terminal-type (optioneel)	Dit kan **xterm** zijn (standaard) of **VT100**.
Keepalive (optioneel)	Het aantal seconden tussen ieder verzonden pakket om te voorkomen dat een niet-actieve sessie wordt gestopt. Dit kan elk getal zijn tussen **0** en **300**. Met **0** wordt het actief houden uitgeschakeld (standaard).
Jumpgroep	De codenaam van het team waarmee deze jumpsnelkoppeling moet worden geassocieerd. ***Opmerking:*** *Bij gebruik van de importmethode kan een jumpsnelkoppeling niet met een persoonlijke Jumpgroep worden geassocieerd.*
Tag (optioneel)	U kunt uw jumpsnelkoppelingen in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw jumpsnelkoppelingen toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.

Veld	Beschrijving
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot deze jumpsnelkoppeling te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op deze jumpsnelkoppeling beschikbaar zijn.

Eindpunt-analyse: Rapporteer open poorten op eindpunten

Configuratie eindpunt-analyse

Eindpunt-analyse inschakelen

Als deze optie is ingeschakeld, dan worden eenmaal per dag open poorten op alle jumpsnelkoppelingen gescand.

TCP-poorten

Voer de TCP-poorten in die moeten worden gescand. Voer meerdere poortnummers in, gescheiden door komma's, of voer een bereik poortnummers in door het laagste en het hoogste poortnummer in te voeren, gescheiden door een streepje.

UDP-poorten

Voer de UDP-poorten in die moeten worden gescand. Voer meerdere poortnummers in, gescheiden door komma's, of voer een bereik poortnummers in door het laagste en het hoogste poortnummer in te voeren, gescheiden door een streepje.

Rapport eindpunt-analyse

Type jumpsnelkoppeling

Selecteer uit het vervolgkeuzemenu het type jumpsnelkoppeling waar u een rapport over wilt hebben.

Jumpoint

U kunt de resultaten verder verfijnen door alleen jumpsnelkoppelingen te selecteren die een verbinding via een geselecteerd Jumpoint hebben.

Open poorten opnemen die al zijn gemarkeerd als verwacht

Verfijn de resultaten verder door poorten uit te sluiten waarvoor u al hebt aangegeven dat u verwacht dat deze open zijn.

Resultaten eindpunt-analyse

Bekijk de open poorten die zijn gevonden op de op de vorige pagina gespecificeerde eindpunten. U kunt poorten aangeven waarvan u verwacht dat deze open zijn zodat deze in toekomstige rapporten uit zijn gefilterd. U kunt ook voor alle poorten aangeven dat u niet verwacht dat ze open zijn.

Toegangsconsole

Instellingen van toegangsconsole: Standaard instellingen van toegangsconsole beheren

Instellingen van toegangsconsole beheren

U kunt de standaard instellingen van de toegangsconsole voor al uw gebruikers instellen en zo een consistente gebruikerservaring voor de toegangsconsole toepassen voor efficiëntere teams. U kunt instellingen afdwingen, toestaan dat de instellingen door de gebruiker worden overschreven of de instellingen onbeheerd laten. Als u **Onbeheerd** selecteert, dan worden de Bomgar standaard instellingen ernaast weergegeven zodat u kunt afwegen of u het echt wilt.

Bij elke instelling waarvoor u **Inschakelen** of **Uitschakelen** selecteert, wordt een keuzevakje weergegeven waarmee u kunt aangeven of de instelling wordt afgedwongen. Afgedwongen instellingen worden effectief als de gebruiker de volgende keer inlogt. Ze kunnen niet in de console worden geconfigureerd. Niet-afgedwongen instellingen kunnen door een gebruiker worden overschreven via het venster Instellingen in de toegangsconsole. Een afgedwongen instelling kan alleen worden overschreven als de beheerder in de /login beheeinterface het vinkje in het keuzevakje **Geforceerd** voor die instelling weghaalt.

Kies de instellingen die u als standaard voor al uw gebruikers wilt en klik op de knop **Opslaan** onderaan de pagina.

NB: opgeslagen instellingen worden pas effectief als op de console wordt ingelogd. Zelfs als u de instellingen opslaat en toepast door op de knop **Nu toepassen** onderaan de pagina te klikken, waarover later meer, gebruikt de gebruiker de nieuwe instellingen pas als hij of zij inlogt.

Als u bijvoorbeeld standaard instellingen voor nieuwe gebruikers wilt instellen maar de instellingen voor bestaande gebruikers ongewijzigd wilt laten, dan kunt u uw beheerde instellingen opslaan maar niet toepassen. Op deze manier word bij iedere nieuwe sessie waarbij op de toegangsconsole wordt ingelogd, uw nieuwe beheerde standaard instellingen van kracht. Voor bestaande gebruikers worden de afgedwongen instellingen de volgende keer dat zij inloggen van kracht, maar alle andere instellingen blijven ongewijzigd.

Algemene instellingen

Spellingcontrole ingeschakeld

Vanuit de sectie **Algemene instellingen** kunt u kiezen om voor chat de spellingcontrole aan of uit te zetten. Momenteel is spellingcontrole alleen beschikbaar voor Amerikaans Engels.

Instelbaar kantlijnartikel voor sessie

Kies of u wilt dat het pictogram voor het sessiemenu wordt weergegeven, of het kantlijnartikel kan worden losgekoppeld en of de widgets op het kantlijnartikel voor de sessie een andere volgorde en grootte kunnen krijgen.

Waarschuwingen :: Chatberichten

Hoorbare waarschuwingen - laat een geluid horen als een chatbericht wordt ontvangen

Kies of er een geluid moet worden afgespeeld als de gebruiker een chatbericht ontvangt. Als een gebruiker niet beheerd is of als deze ingeschakeld en niet geforceerd is, dan mag hij of zij een aangepast geluid in WAV-formaat aanwijzen met een maximale grootte van 1 MB.

Visuele waarschuwingen - laat het toepassing-pictogram knipperen als een chatbericht wordt ontvangen

Kies of het pictogram voor de toepassing moet knipperen als de gebruiker een chatbericht ontvangt.

Statusberichten in chat-vensters van team weergeven

Kies of statusberichten in de teamchat worden meegenomen, zoals het in- of uitloggen van gebruikers, of alleen de tussen teamleden verzonden chats.

Pop-up-meldingen

Teamwachtrijen

Kies of een gebruiker een pop-up-melding moet ontvangen voor in een teamchat ontvangen chatberichten.

Toegangssessies

Kies of een gebruiker een pop-up-melding moet ontvangen voor in een toegangssessie ontvangen chatberichten.

Waarschuwingen :: Wachtrij-waarschuwingen

Hoorbare waarschuwingen - laat een geluid horen als een sessie een wachtrij binnenkomt

Kies of een geluid moet worden afgespeeld als er een sessie in een van de wachtrijen van de gebruiker komt.

Pop-up-meldingen

Pop-up-meldingen verschijnen onafhankelijk van de toegangsconsole en bovenop andere vensters. Als de pop-up-melding is ingeschakeld en niet afgedwongen is of onbeheerd wordt gelaten, dan kan de gebruiker kiezen hoe hij of zij pop-up-meldingen wil ontvangen.

Persoonlijke wachtrij - gedeelde sessies

Kies of een gebruiker een pop-up-melding moet ontvangen voor gedeelde sessies in deze wachtrij.

Teamwachtrijen - gedeelde sessies

Kies of een gebruiker een pop-up-melding moet ontvangen voor gedeelde sessies in deze wachtrij.

Pop-up-gedrag - locatie en duur

Stel de standaard locatie en duur in voor pop-up-meldingen.

Toegangssessies :: Automatisch gedrag

Automatische aanvraag Scherm delen

Kies of u wilt dat in de sessies van uw gebruikers scherm delen actief is bij het begin.

Automatisch loskoppelen

Kies of u sessies als tabbladen in de toegangsconsole wilt openen of automatisch sessies los te koppelen en in nieuwe vensters weer te geven.

Automatisch opwaarderen van Jump-pogingen in het lokale netwerk

Kies of een client op een eindpunt automatisch moet worden opgewaardeerd om als systeemservice te worden uitgevoerd als de gebruiker een Jump in het lokale netwerk uitvoert.

Prompt om op te waarderen als beveiligd bureaublad op het eindpunt is ingeschakeld

In situaties waar gebruikers problemen kunnen tegenkomen doordat een gebruiker een beveiligd bureaublad heeft, kunt u toestaan dat uw gebruikers een prompt krijgen om op te waarderen zodat zij bij het begin van de sessie met beheerdersrechten werken.

Toegangssessies :: Gereedschappen

Scherm delen

Standaardkwaliteit

Stel de standaard kwaliteit in voor sessies met scherm delen.

Standaardschaal

Stel de standaard afmetingen in voor sessies met scherm delen.

Automatisch naar volledig scherm wanneer scherm delen begint

Als scherm delen begint, dan kan de gebruiker automatisch naar volledig scherm gaan.

Kantlijnartikel automatisch invouwen wanneer volledig scherm wordt gebruikt

Als de sessie met scherm delen naar volledig scherm gaat, dan kan de chatbalk automatisch worden ingeklapt.

Opdrachtshell

Aantal regels beschikbaar in opdrachtgeschiedenis

U kunt het aantal regels instellen dat in de historie van de opdrachtshell wordt opgeslagen. De standaard waarde is 500 regels.

Opslaan

Klik op **Opslaan** om alle profielinstellingen op te slaan die u hebt geconfigureerd. Het bevestigingsbericht **Opslaan instellingenprofiel geslaagd** verschijnt bovenaan de pagina. Alle gebruikers die op de toegangsconsole inloggen nadat u een nieuw profiel hebt opgeslagen, krijgen de nieuwe instellingen als standaard instellingen.

Beheerde instellingen van toegangsconsole toepassen

Nu toepassen

Als u de standaard instellingen op al uw gebruikers van toepassing wilt laten zijn, klik dan op **Nu toepassen**. Er verschijnt bovenaan de pagina een bevestigingsbericht **Opslaan instellingenprofiel geslaagd**.

Nadat u de nieuwe instellingen op alle gebruikers van toepassing hebt gemaakt, krijgen de gebruikers een waarschuwingsdialoog om te bevestigen dat de nieuwe instellingen van toepassing zijn de eerstvolgende keer dat zij op de toegangsconsole inloggen nadat u de instellingen van toepassing hebt gemaakt. In de dialoog worden zij gewaarschuwd dat hun instellingen zijn gewijzigd en zij krijgen een prompt met de optie de dialoog te bevestigen of hun instellingenvenster voor de toegangsconsole te openen om de wijzigingen te bekijken.

Aanpasbare koppelingen: URL-snelkoppelingen naar de toegangsconsole toevoegen

Aanpasbare koppelingen

Maak koppelingen naar sites aan waar gebruikers tijdens sessies toegang toe kunnen hebben.Voorbeelden zijn een koppeling naar een kennisbank met zoekmogelijkheden, zodat gebruikers de mogelijkheid hebben om een oplossing voor een probleem op het eindpuntsysteem op te zoeken of een CRM-systeem.

Hier aangemaakte koppelingen worden via de knop **Koppelingen** op de toegangsconsole beschikbaar gesteld.

Nieuwe aanpasbare koppeling aanmaken, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Aanpasbare koppelingen :: Toevoegen of bewerken

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

URL

Voeg de URL toe waar deze aanpasbare koppeling naar moet verwijzen. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Standaard scripts: Scripts aanmaken voor sessies met scherm delen of met opdrachtshell

Standaard scripts

Maak aangepaste scripts aan om te gebruiken in sessies met scherm delen en opdrachtshell. Het script wordt in de interface van scherm delen of opdrachtshell weergegeven terwijl het wordt uitgevoerd. Als u een script in de interface voor scherm delen uitvoert, dan wordt het uitgevoerde script op het externe beeldscherm weergegeven.

Filteren op

Filter uw weergave door in de vervolgkeuzelijst bovenaan de pagina een categorie of team te selecteren.

Nieuw standaard script toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Standaard script :: Toevoegen of bewerken

Scriptnaam

Maak een unieke naam aan om te helpen dit object te identificeren. Deze naam moet de gebruikers helpen het script te vinden dat zij willen uitvoeren.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit object samen te vatten. De beschrijving wordt bij de prompt weergegeven om te bevestigen dat de gebruiker het geselecteerde script wil uitvoeren.

Opdrachtenreeks

Schrijf de serie opdrachten. Scripts moeten in opdrachtregel formaat worden geschreven, net zoals u een batchbestand of shellscript schrijft. Let op dat alleen de laatste regel interactief kan zijn: u kunt niet middenin een script om invoer vragen.

In het script kunt u aan een hulpbronbestand refereren door middel van **“%RESOURCE_FILE%”**. Let er daarbij op dat u de aanhalingstekens niet vergeet. Let op dat de opdrachtenreeks hoofdlettergevoelig is.

U kunt toegang krijgen tot de tijdelijke map van het hulpbronbestand door **%RESOURCE_DIR%** te gebruiken. Als u een script uitvoert met een bijbehorend hulpbronbestand, dan wordt dat bestand tijdelijk naar de computer van de klant geüpload.

Teams

Selecteer welke teams dit item moeten kunnen gebruiken.

Categorieën

Selecteer de categorie waaronder dit item in de lijst moet worden opgenomen.

Hulpbronbestand

U kunt een hulpbronbestand selecteren dat bij dit script hoort.

Opwaarderingsmodus

Selecteer of dit script alleen in opgewaardeerde modus mag worden uitgevoerd, alleen in niet-opgewaardeerde modus of in beide modi.

Categorieën

Categorie toevoegen, verwijderen

Maak een nieuwe categorie aan of verwijder een bestaande categorie.

Bronnen

Uploaden

Voeg eventuele hulpbronbestanden toe waar u vanuit uw scripts toegang toe wilt hebben. U mag maximaal 100 MB naar uw map met hulpbronbestanden uploaden.

Verwijderen

Verwijder een bestaand hulpbronbestand.

Speciale acties: Aangepaste speciale acties aanmaken

Speciale acties aanpassen

Maak aangepaste speciale acties aan om uw processen sneller te laten verlopen. U kunt aangepaste speciale acties aanmaken voor Windows, Mac en Linux systemen.

Nieuwe aangepaste speciale actie toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Speciale actie toevoegen of bewerken

Naam actie

Maak een unieke naam aan om te helpen dit object te identificeren. Een gebruiker kan tijdens een sessie deze naam in de vervolgkeuzelijst speciale acties zien.

Opdracht

Voer in het veld **Opdracht** het volledige pad in van de toepassing die u wilt uitvoeren. Gebruik geen aanhalingstekens, deze worden automatisch toegevoegd indien nodig. Windows systemen maken gebruik van de opgegeven macro's. Als de opdracht op het externe systeem niet kan worden gevonden, dan verschijnt deze aangepaste speciale actie niet in de lijst speciale acties voor de gebruiker.

Argumenten

Als de opgegeven opdracht argumenten op de opdrachtregel accepteert, dan kunt u die argumenten vervolgens invoeren. In argumenten mogen, indien nodig, aanhalingstekens worden gebruikt en in argumenten voor Windows mogen de geleverde macro's worden gebruikt. Voor hulp met Windows-argumenten kunt u zoeken op “command line switches" (switches voor opdrachtregels) op msdn.microsoft.com.

Bevestigen

Als u het vakje **Bevestigen** aanvinkt, dan wordt aan gebruikers gevraagd te bevestigen dat zij deze speciale actie willen uitvoeren voordat de speciale actie daadwerkelijk wordt uitgevoerd. Anders wordt, wanneer de aangepaste speciale actie tijdens een sessie in het menu wordt geselecteerd, die speciale actie direct uitgevoerd.

Opgewaardeerd uitvoeren

Door deze optie aan te vinken verschijnt deze speciale actie alleen als de client op het eindpunt in opgewaardeerde modus wordt uitgevoerd. Als u een aangepaste actie in opgewaardeerde modus uitvoert, dan wordt u gevraagd om die actie als de systeemgebruiker uit te voeren of om inloggegevens te verstrekken voor een ander geldig account op het externe systeem.

Instellingen speciale acties

Ingebouwde speciale acties weergeven

Als u de door Bomgar geleverde standaard speciale acties inschakelt, dan moet u de optie **Ingebouwde speciale acties weergeven** aanvinken. Als u daarentegen alleen uw eigen speciale acties wilt inschakelen, dan mag u deze optie niet aanvinken.

Opmerking: *De speciale actie* ***Windows beveiliging (Ctrl-Alt-Del)*** *kan niet worden uitgeschakeld. Ook worden als u de ingebouwde speciale acties uitschakelt, de standaard speciale acties voor mobiele apparaten niet uitgeschakeld.*

Gebruikers en beveiliging

Gebruikers: Accountmachtigingen toevoegen voor een gebruiker of beheerder

Gebruikersaccounts

Bekijk informatie over alle gebruikers die toegang tot uw Bomgar Box hebben, inclusief alle lokale gebruikers en de gebruikers die toegang hebben via integratie met een beveiligingsprovider.

Nieuwe gebruiker aanmaken, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object. U kunt uw eigen account niet verwijderen.

Synchroniseren

Synchroniseer de gebruikers en groepen die met een externe beveiligingsprovider geassocieerd zijn. De synchronisatie wordt eenmaal per dag automatisch uitgevoerd. Als u op deze knop klikt, wordt de synchronisatie handmatig uitgevoerd.

Zoeken

Doorzoek gebruikersaccounts op basis van gebruikersnaam en schermnaam.

Resetten

Als de gebruiker een of meer mislukte pogingen heeft gedaan om in te loggen, dan moet u op de knop **Resetten** naast zijn of haar naam klikken om het aantal terug te zetten op 0.

Gebruiker :: Toevoegen of bewerken

Gebruikersinstellingen

Gebruikersnaam

Unieke identificatie om in te loggen.

Schermnaam

De naam van de gebruiker zoals deze in teamchats, rapporten e.d. wordt weergegeven.

E-mailadres

Stel het e-mailadres in waarnaar e-mailkennisgevingen moeten worden verzonden, zoals het opnieuw instellen van het wachtwoord of waarschuwingen over uitgebreide beschikbaarheid-modus.

Voorkeurstaal voor e-mail

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Wachtwoord

Wachtwoord dat samen met de gebruikersnaam wordt gebruikt om in te loggen. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

E-mail wachtwoord naar gebruiker

Een automatische e-mail naar de gebruiker verzenden die zijn of haar nieuwe wachtwoord bevat. Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen. Voor deze functie is een geldige SMTP-configuratie voor uw apparaat vereist. U kunt deze instellen op de pagina **/login > Beheer > E-mailconfiguratie**.

Moet wachtwoord opnieuw instellen bij volgende login

Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen.

Wachtwoord vervalt op

Hierdoor vervalt het wachtwoord na een bepaalde datum of vervalt het nooit.

Beveiligingsvraag en beveiligingsantwoord

Een gebruiker kan met de beveiligingsvraag en het antwoord erop een vergeten wachtwoord resetten nadat hij of zij het juiste antwoord op de vraag heeft gegeven. Wachtwoorden mogen alleen worden gereset als **Wachtwoord resetten inschakelen** aangevinkt is op de pagina **Beheer > Beveiliging**. Beheerders kunnen hun wachtwoorden met behulp van de beveiligingsvraag niet opnieuw instellen.

Lidmaatschappen van groepsbeleid

Overzicht van de groepsbeleidslijnen waar deze gebruiker toe behoort, met koppeling naar de pagina **Groepsbeleid** of de beleidslijnen zelf.

Teamlidmaatschappen

Overzicht van de teams waar de gebruiker toe behoort, met koppeling naar de pagina **Teams** of de teams zelf.

Accountinstellingen

Laatste verificatiedatum

De datum en het tijdstip waarop deze gebruiker de laatste keer heeft ingelogd.

Inlogcode voor e-mail

Hierdoor wordt meervoudige verificatie toegestaan. Gebruikers ontvangen telkens wanneer zij op de /loging beheerinterface op de toegangsconsole inloggen een e-mail met een unieke verificatiecode, zowel op een computer als op een mobiel apparaat. Als de code drie keer achtereen onjuist wordt ingevoerd, dan moeten de gebruikers hun inloggegevens opnieuw invoeren en een nieuwe e-mailcode invoeren.

Account vervalt op

Hierdoor vervalt het account na een bepaalde datum of vervalt het nooit.

Account uitgeschakeld

Hierdoor wordt het account uitgeschakeld zodat de gebruiker niet kan inloggen. Als een account wordt uitgeschakeld, wordt het NIET verwijderd.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Machtigingen

Beheerder

Hoerdoor krijgt de gebruiker volledige beheerdersrechten.

Mag wachtwoorden instellen

Hierdoor kan de gebruiker wachtwoorden instellen en accounts ontgrendelen voor lokale gebruikers die geen beheerder zijn.

Mag Jumpoints bewerken

Hierdoor mogen gebruikers Jumpoints aanmaken of bewerken. Deze optie heeft geen invloed op de mogelijkheid voor de gebruikers om via Jumpoints toegang tot externe computers te krijgen. Dat wordt via beleid op Jumpoint- of groepsniveau geconfigureerd.

Toestemmingen voor toegangssessierapportage: Mag rapporten van toegangssessies bekijken

Hierdoor kan de gebruiker rapporten maken over activiteiten tijdens toegangssessies, waarbij hij of zij alleen sessies kan bekijken waarvan hij of zij de primaire sessie-eigenaar was, alleen sessies waarbij een van zijn of haar teams het primaire team was, alleen sessies waarin een van zijn of haar teamleden de primaire sessie-eigenaar was of alle sessies.

Mag opnames van toegangssessies bekijken

Hierdoor kan een gebruiker opnames bekijken van sessies met scherm delen en van sessies met opdrachtshell.

Mag rapportage API gebruiken

Hierdoor kunnen de inloggegevens van de gebruiker worden gebruikt om via de API XML-rapporten op te halen.

Mag opdracht API gebruiken

Hierdoor kunnen de inloggegevens van de gebruiker worden gebruikt om via de API opdrachten te geven.

Mag teams bewerken

Hierdoor kunnen gebruikers teams aanmaken of bewerken.

Mag standaard scripts bewerken

Hierdoor kan de gebruiker standaard scripts aanmaken of bewerken die worden gebruikt in sessies met scherm delen of met opdrachtshell.

Mag aangepaste links bewerken

Hierdoor kan de gebruiker aanpasbare koppelingen aanmaken of bewerken.

Toegangsmachtigingen

Toegang

Toestemming voor toegang tot eindpunten

Hierdoor mag de gebruiker de toegangsconsole gebruiken om sessies uit te voeren. Als toegang tot een eindpunt is ingeschakeld, dan zijn er ook opties beschikbaar die betrekking hebben op toegang tot een eindpunt.

Sessiebeheer

Mag sessies delen met teams waarvan hij/zij geen deel uitmaakt

Hierdoor kan de gebruiker behalve zijn of haar teamleden ook een minder beperkte groep gebruikers uitnodigen om sessies te delen. Samen met de machtiging Uitgebreide beschikbaarheid vormt deze machtiging een uitbreiding van de mogelijkheden om sessies te delen.

Mag externe gebruikers uitnodigen

Hierdoor kan de gebruiker een gebruiker van een derde partij uitnodigen eenmalig aan een sessie deel te nemen.

Mag modus Uitgebreide beschikbaarheid inschakelen

Hierdoor kan de gebruiker e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen, ook als hij of zij niet op de toegangsconsole is ingelogd.

Mag de externe sleutel bewerken

Staat gebruikers toe om de externe sleutel te wijzigen vanaf het informatiedeelvenster van een sessie binnen de toegangsconsole.

Scherm delen van gebruiker tot gebruiker

Mag scherm tonen aan andere gebruikers

Hierdoor kan een gebruiker zijn of haar scherm delen met een andere gebruiker zonder dat de ontvanger aan een sessie hoeft aan te melden. Deze optie is zelfs beschikbaar als de gebruiker niet in een sessie is.

Mag besturing geven tijdens tonen van scherm aan andere gebruikers

Hierdoor kan de gebruiker tijdens scherm delen de besturing over muis en toetsenbord aan de gebruiker geven die zijn of haar scherm bekijkt.

Jump-technologie

Toegestane Jump-methodes: Mag sessies opstarten via Jump-clients die een van de volgende Jump-methodes gebruiken:

Hierdoor kan de gebruiker een Jump uitvoeren naar computers via **Jump-clients**, **Lokale Jump op het lokale netwerk**, **Externe Jump via een Jumpoint**, **Bureaublad op afstand via een Jumpoint** en/of **Shell Jump via een Jumpoint**.

Machtigingen voor jumpsnelkoppelingen: Mag sessies van alle jumpsnelkoppelingen binnen het systeem starten

Hierdoor mag de gebruiker een Jump uitvoeren naar externe computers in alle Jumpgroepen van het team.

Mag jumpsnelkoppelingen implementeren, verwijderen en wijzigen in de volgende Jumpgroepen:

Hierdoor kan de gebruiker sessies vastspelden, groepen instellen en commentaar aan jumpsnelkoppelingen toevoegen voor zijn of haar persoonlijke Jumpgroep, voor Jumpgroepen van een team en van teamleden of voor alle Jumpgroepen, inclusief de Jumpgroepen die aan teams zijn toegewezen waar de gebruiker niet toe behoort en aan de persoonlijke Jumpgroep van elke gebruiker.

Mag de met jumpsnelkoppelingen geassocieerde sessiebeleidslijnen wijzigen

Hierdoor kan de gebruiker het sessiebeleid instellen dat een jumpsnelkoppeling moet gebruiken. Het wijzigen van het sessiebeleid kan van invloed zijn op de machtigingen in de sessie.

Sessietoestemmingen

Stel de prompts en de machtigingsregels in die voor de sessies van deze gebruiker moeten gelden. Kies een bestaand sessiebeleid of definieer aangepaste machtigingen voor deze gebruiker. Als u **Niet gedefinieerd** specificeert, dan wordt het algemene standaard beleid gebruikt. Deze machtigingen kunnen door een beleid met hogere prioriteit worden overschreven.

Beschrijving

Bekijk de omschrijving van een vooraf gedefinieerd beleid voor sessietoestemming.

Scherm delen

Scherm delen

Hierdoor kan de gebruiker het externe scherm bekijken of besturen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.

Opmerking: *Deze functie geldt alleen voor Windows en Linux besturingssystemen en geldt niet voor sessies met bureaublad op afstand (RDP).*

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar één of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Opmerking: *Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.*

Toegestane eindpuntbeperkingen

Stel in of de gebruiker de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.

Mag inloggen met inloggegevens van een beheerder van verificatiegegevens voor een eindpunt

Activeer een verbinding van een gebruiker naar de beheerder van eindpunt-verificatiegegevens vanaf uw bestaande wachtwoord-opslagplaatsen of -kluizen.

Voor gebruik van Beheerder van verificatiegegevens voor eindpunt is een aparte onderhoudsovereenkomst met Bomgar vereist. Als een onderhoudsovereenkomst eenmaal is afgesloten, mag u de benodigde middleware vanuit het Bomgar self-service center downloaden.

Opmerking: *In eerdere versies dan 15.2 is deze functie alleen beschikbaar in sessies die vanaf een opgewaardeerde Jump-client op Windows® zijn gestart. Vanaf versie 15.2 mag u ook een beheerder van eindpunt-verificatiegegevens gebruiken in sessies met externe Jump, met Microsoft® bureaublad op afstand of met Shell Jump. U kunt deze functie ook gebruiken in een sessie met scherm delen op een Windows® systeem door gebruik te maken van de speciale actie Uitvoeren als.*

Annotaties

Hierdoor kan de gebruiker gereedschappen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Bestandsoverdracht

Bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.

Opdrachtshell

Opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden

overschreven door een beleid met hogere prioriteit.

Systeeminformatie

Systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer zien. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toestemming tot gebruik van systeeminformatie-acties

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

Register-toegang

Register-toegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

Andere hulpprogramma's

Standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Opwaardering

Hierdoor kan de gebruiker proberen de eindpunt-client op te waarderen zodat deze met beheerdersrechten op het externe systeem kan worden uitgevoerd. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Inlogschema

Beperk inloggen van gebruiker aan de hand van het volgende rooster

Stel een rooster in om te definiëren wanneer gebruikers op de toegangsconsole in kunnen loggen. Stel de tijdzone in die u voor dit rooster wilt gebruiker en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als bijvoorbeeld de begintijd is ingesteld op 08:00 uur en de eindtijd op 17:00 uur, dan kan een gebruiker op elk tijdstip in deze periode inloggen en kan blijven doorwerken tot na de eindtijd. De gebruiker kan echter na 17:00 uur niet opnieuw inloggen.

Forceer uitloggen als het schema inloggen niet toestaat

Als strengere toegangscontrole is vereist, dan moet u deze optie aanvinken. Hierdoor wordt de gebruiker geforceerd op de geplande eindtijd uit te loggen. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd. Wanneer de gebruiker uitgelogd wordt, volgen eventuele eigen sessies de sessieterugval-regels.

Rapport Gebruikersaccount

Exporteer gedetailleerde informatie over uw gebruikers voor controledoeleinden. Verzamel gedetailleerde informatie over alle gebruikers, gebruikers van een bepaalde beveiligingsprovider of alleen lokale gebruikers. De verzamelde informatie bevat gegevens weergegeven onder de knop “Gegevens weergeven” plus groepsbeleids- en teamlidmaatschappen en machtigingen.

Gebruikersaccounts om wachtwoorden opnieuw in te stellen: Gebruikers toestaan om wachtwoorden te beheren

Gebruikersaccounts

Beheerders kunnen via gebruikersmachtiging de taak van het resetten van de wachtwoorden van lokale gebruikers en vergrendelde gebruikersaccounts aan bevoorrechte gebruikers delegeren, zonder volledige beheerdersrechten toe te kennen. Gebruikers kunnen nog steeds hun eigen wachtwoord resetten.

Opmerking: *Beheerders met de machtiging* ***Mag wachtwoorden instellen*** *zien geen verschil in de gebruikersinterface.*

Als een bevoorrechte gebruiker die geen beheerdersrechten heeft naar de pagina **Gebruikers en beveiliging > Gebruikers** in de beheerders /login interface gaat, dan ziet hij of zij een beperkte weergave van het scherm **Gebruikers** met **Wachtwoord wijzigen** koppelingen voor gebruikers zonder beheerdersrechten. De bevoorrechte gebruiker kan geen gebruikersaccounts bewerken of verwijderen. Bevoorrechte gebruikers mogen geen wachtwoorden van beheerders of van gebruikers van beveiligingsproviders resetten.

Zoeken

Doorzoek gebruikersaccounts op basis van gebruikersnaam en schermnaam.

Resetten

Als de gebruiker een of meer mislukte pogingen heeft gedaan om in te loggen, dan moet u op de knop **Resetten** naast zijn of haar naam klikken om het aantal terug te zetten op 0.

Wachtwoord veranderen

Wijzig het wachtwoord van een gebruiker die geen beheerder is.

Gebruiker :: Wachtwoord veranderen

Gebruikersnaam

Unieke identificatie om in te loggen. Dit veld kan niet worden bewerkt.

Schermnamen

De naam van de gebruiker zoals deze in teamchats, rapporten e.d. wordt weergegeven. Dit veld kan niet worden bewerkt.

E-mailadres

Het e-mailadres waarheen e-mails met kennisgevingen worden verzonden, zoals het resetten van wachtwoorden of waarschuwingen over uitgebreide beschikbaarheid-modus. Dit veld kan niet worden bewerkt.

Opmerkingen

Opmerkingen over het account. Dit veld kan niet worden bewerkt.

Wachtwoord

Het nieuwe wachtwoord dat aan dit gebruikersaccount wordt toegekend. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

E-mail wachtwoord naar gebruiker

Een automatische e-mail naar de gebruiker verzenden die zijn of haar nieuwe wachtwoord bevat. Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen. Voor deze functie is een geldige SMTP-configuratie voor uw apparaat vereist. U kunt deze instellen op de pagina **/login > Beheer > E-mailconfiguratie**.

Moet wachtwoord opnieuw instellen bij volgende login

Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen.

Toegangsuitnodiging: Profielen aanmaken om externe gebruikers in sessies uit te nodigen

E-mailuitnodiging openen

Een bevoorrechte gebruiker kan met een toegangsuitnodiging een externe gebruiker uitnodigen om eenmalig een sessies bij te wonen. Als de gebruiker de uitnodiging maakt, dan moet hij of zij een beveiligingsprofiel selecteren om te bepalen welk niveau privileges de externe gebruiker moet krijgen. Beveiligingsprofielen voor toegangsuitnodigingen worden op de pagina **Gebruikers en beveiliging > Sessiebeleidslijnen** als sessiebeleidslijnen geconfigureerd en moeten worden ingeschakeld voor gebruik in toegangsuitnodigingen.

De e-mailuitnodiging wordt naar externe gebruikers verzonden als u hen uitnodigt een sessie bij te wonen.

Onderwerp

Pas het onderwerp van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Body

Pas de inhoud van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Beveiligingsproviders: Inloggen via LDAP, Active Directory, RADIUS en Kerberos activeren

Beveiligingsproviders

U kunt uw Bomgar Box configureren om gebruikers tegen bestaande LDAP, RADIUS of Kerberos servers te verifiëren en om machtigingen toe te kennen op basis van eerdere instellingen voor hiërarchie en groepen die al in uw servers zijn gespecificeerd. Kerberos ondersteunt eenmalige aanmelding, RSA en andere verificatiemechanismes voor meervoudige verificatie via RADIUS bieden een extra beveiligingsniveau.

Provider aanmaken

Maak een configuratie voor een nieuwe beveiligingsprovider aan. Selecteer uit de vervolgkeuzelijst om een LDAP-provider, een RADIUS-provider of een Kerberos-provider aan te maken.

Logboek bekijken

Bekijk de statushistorie voor een verbinding met een beveiligingsprovider.

Synchronisatie

Synchroniseer de gebruikers en groepen die met een externe beveiligingsprovider geassocieerd zijn. De synchronisatie wordt eenmaal per dag automatisch uitgevoerd. Als u op deze knop klikt, wordt de synchronisatie handmatig uitgevoerd.

Uitschakelen

Schakel de verbinding met deze beveiligingsprovider uit. Dit is nuttig voor gepland onderhoud, als u wilt dat een server offline is maar niet verwijderd is.

Bewerken, verwijderen

Wijzig een bestaand object of verwijder een bestaand object.

Kopie aanmaken

Maak een kopie van een bestaande configuratie van een beveiligingsprovider aan. Deze wordt als een beveiligingsprovider op het hoogste niveau toegevoegd en niet als onderdeel van een cluster.

Node dupliceren

Maak een kopie van een bestaande configuratie van een geclusterde beveiligingsprovider aan. Deze wordt als nieuwe node aan dezelfde cluster toegevoegd.

Tot cluster bijwerken

Upgrade een beveiligingsprovider tot een geclusterde beveiligingsprovider. Kopieer een bestaande node om meer beveiligingsproviders aan deze cluster toe te voegen.

Volgorde veranderen

Klik op deze knop om beveiligingsproviders te slepen en neer te zetten om de prioriteiten ervan in te stellen. U kunt servers binnen een cluster slepen en neerzetten en clusters kunnen als geheel worden gesleept en neergezet. Klik op **Volgorde opslaan** om de wijzigingen in de prioriteiten te effectueren.

Beveiligingsproviders :: Bewerken: LDAP

Algemene instellingen

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

Ingeschakeld: Deze provider is ingeschakeld

Indien dit veld is aangevinkt, kan uw Bomgar Box naar deze beveiligingsprovider zoeken als een gebruiker probeert in te loggen. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Schermnamen van gebruikers: Houd de schermnaam gesynchroniseerd met het systeem op afstand

Met deze waarden wordt bepaald welke velden gebruikt moeten worden voor de privé- en publieke schermnamen van de gebruiker.

Synchronisatie: LDAP-objectcache inschakelen

Als deze optie is aangevinkt, dan worden LDAP-objecten die voor het apparaat zichtbaar zijn, elke nacht of, indien gewenst handmatig, gecachet en gesynchroniseerd. Bij gebruik van deze optie worden er minder verbindingen met de LDAP-server voor beheerdoeleinden gemaakt zodat potentieel de snelheid en efficiency omhoog gaan.

Als deze optie niet is aangevinkt, dan komen wijzigingen op de LDAP-server direct beschikbaar zonder de noodzaak tot synchronisatie. Maar als u via de beheerinterface wijzigingen maakt in gebruikersbeleidslijnen, dan worden, voor zover noodzakelijk, enkele kortstondige verbindingen met de LDAP-server gemaakt.

Bij providers die voorheen de synchronisatie in hadden geschakeld en de synchronisatie uitschakelen door het vinkje bij de synchronisatie-optie weg te halen, worden alle gecachete records verwijderd die op dat moment niet in gebruik zijn.

Autorisatie-instellingen

Groep opzoeken

U kunt ervoor kiezen deze beveiligingsprovider alleen voor gebruikersverificatie te gebruiken, alleen voor het opzoeken van groepen of voor beide doeleinden.

Standaard groepsbeleid *(Alleen zichtbaar als gebruikersverificatie is toegestaan)*

Elke gebruiker die tegen een externe server wordt geverifieerd, moet een lid van tenminste één groepsbeleid zijn om op uw Bomgar Box te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login interface ofwel de toegangsconsole. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.

Opmerking: *Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.*

Instellingen voor verbinding

Hostnaam

Voer de hostnaam in van de server waar uw externe adreslijstarchief staat.

Opmerking: *Als u **LDAPS** of **LDAP met TLS** gebruikt, dan moet de hostnaam overeenkomen met de in het publieke SSL-certificaat van uw LDAP-server gebruikte onderwerpnaam of met de DNS-component van de alternatieve onderwerpnaam.*

Poort

Specificeer de poort voor uw LDAP-server. Dit is meestal poort **389** voor LDAP of poort **636** voor LDAPS. Bomgar ondersteunt ook een globale catalogus over poort **3268** voor LDAP of **3269** voor LDAPS.

Versleuteling

Selecteer het type versleuteling dat moet worden gebruikt voor communicatie met de LDAP-server. Om beveiligingsredenen wordt **LDAPS** of **LDAP met TLS** aanbevolen.

Opmerking: *Standaard LDAP verzendt en ontvangt gegevens ongecodeerd van de LDAP-server en stelt zo mogelijk vertrouwelijke informatie over het gebruikersaccount aan packet sniffing bloot. Zowel LDAPS als LDAP met TLS versleutelen de verzonden gegevens waardoor deze methodes aanbevolen worden boven standaard LDAP. LDAP met TLS gebruikt de functie StartTLS om een verbinding met LDAP ongecodeerd op te zetten maar waardeert deze verbinding vervolgens op tot een versleutelde verbinding. LDAPS zet de verbinding over een versleutelde verbinding op zonder enige tekst ongecodeerd te verzenden.*

Als u **LDAPS** of **LDAP met TLS** selecteert, dan moet u het door uw LDAP-server gebruikte SSL-basiscertificaat uploaden. Dit is nodig om de geldigheid van de server en de beveiliging van de gegevens zeker te stellen. Het basiscertificaat moet de PEM-opmaak hebben.

Opmerking: *Als de onderwerpnaam van het publieke SSL-certificaat van de LDAP-server of de DNS-component van de alternatieve onderwerpnaam niet met de waarde in het veld* ***Hostnaam*** *overeenkomt, dan wordt de provider als onbereikbaar behandeld. U kunt echter een wildcardcertificaat opgeven om meerdere subdomeinen op dezelfde site te certificeren. Zo certificeert bijvoorbeeld een certificaat voor* ****.example.com*** *zowel* ***access.example.com*** *als* ***remote.example.com****.*

Verificatiegegevens binden

Specificeer een gebruikersnaam en wachtwoord waarmee uw Bomgar Box een binding kan maken met en kan zoeken in het LDAP-adreslijstarchief.

Als uw server anonieme binding ondersteunt, dan kunt u ervoor kiezen om een binding te maken zonder een gebruikersnaam en wachtwoord te specificeren. Anonieme binding wordt geacht onveilig te zijn en is op de meeste LDAP-servers standaard uitgeschakeld.

Verbindingsmethode

Als u een extern adreslijstarchief gebruikt in hetzelfde lokale netwerk als uw Bomgar Box, dan kunnen de twee systemen direct met elkaar communiceren. In dat geval hoeft u de optie **Proxy van apparaat via de verbindingsagent** niet aan te vinken en kunt u verder gaan.

Als de twee systemen niet direct met elkaar kunnen communiceren, bijvoorbeeld als uw externe adreslijstserver achter een firewall staat, dan moet u een verbindingsagent gebruiken. Als u de Win32 verbindingsagent downloadt, dan kunnen uw adreslijstserver en uw Bomgar Box met elkaar communiceren via een uitgaande met SSL versleutelde verbinding zonder firewallconfiguratie. De verbindingsagent kan ofwel direct naar de adreslijstserver worden gedownload, ofwel naar een aparte server op hetzelfde netwerk als uw adreslijstserver (aanbevolen).

In het bovenstaande geval moet u **Proxy van apparaat via de verbindingsagent** aanvinken. Maak een **Wachtwoord verbindingsagent** aan om tijdens de installatie van de verbindingsagent te gebruiken. Klik vervolgens op **Verbindingsagent downloaden**, voer het installatieprogramma uit en volg de instructies van de installatiewizard op. Tijdens installatie wordt u gevraagd om de naam van de beveiligingsprovider in te voeren evenals het hier hierboven aangemaakte wachtwoord voor de verbindingsagent.

Type map

Om u te helpen de netwerkverbinding tussen uw Bomgar Box en uw beveiligingsprovider te configureren, kunt u een type map als sjabloon selecteren. Zo worden onderstaande te configureren velden vooraf met standaard gegevens ingevuld, maar die gegevens moeten worden gewijzigd om ze in overeenstemming te brengen met de specifieke configuratie van uw beveiligingsprovider. Active Directory LDAP is het meest gebruikte type server, maar u kunt Bomgar zo configureren dat met de meeste typen beveiligingsproviders kan worden gecommuniceerd.

Instellingen voor cluster *(Alleen zichtbaar voor clusters)*

Selectie-algoritme voor leden

Selecteer de methode waarmee in deze cluster naar nodes wordt gezocht.

Bij **Van boven naar beneden** wordt eerst op de server met de hoogste prioriteit gezocht. Als die server niet beschikbaar is of als het account niet is gevonden, dan wordt op de server met de daarop volgende prioriteit gezocht. Vervolgens wordt in volgorde van aflopende prioriteit op de servers uit de lijst geclusterde servers gezocht tot het account is gevonden of blijkt dat het account niet op een van de gespecificeerde en beschikbare servers bestaat.

Round-robin is bedoeld om de belasting van de verschillende servers in balans te houden. Bij dit algoritme wordt de eerste server waarop wordt gezocht willekeurig gekozen. Als die server niet beschikbaar is of als het account niet is gevonden, dan wordt op een willekeurige andere server gezocht. Vervolgens wordt in willekeurige volgorde op de overige servers uit de lijst geclusterde servers gezocht tot het account is gevonden of blijkt dat het account niet op een van de gespecificeerde en beschikbare servers bestaat.

Wachttijd voor opnieuw proberen

Stel in hoe lang moet worden gewacht nadat een lid van een cluster niet beschikbaar is geworden voordat een nieuwe poging wordt gedaan voor dat lid van die cluster.

Instellingen gebruikersschema

Clusterwaarden overschrijven *(Alleen zichtbaar voor clusternodes)*

Als deze optie niet is aangevinkt, dan worden voor deze clusternode dezelfde schema-instellingen gebruikt als voor de cluster. Als deze optie niet is aangevinkt, dan kunt u hieronder de schema-instellingen wijzigingen.

Basis DN opzoeken

Bepaal het niveau in uw mappenhiërarchie, gespecificeerd door een onderscheiden naam, waar de Bomgar Box moet beginnen naar gebruikers te zoeken. Afhankelijk van de grootte van uw adreslijstarchief en de gebruikers die Bomgar accounts nodig hebben, kunt u de prestaties verbeteren door de specifieke organisatorische eenheid in uw adreslijstarchief aan te wijzen waar toegang toe nodig is. Als u niet zeker weet of gebruikers binnen meerdere organisatorische eenheden actief zijn, kunt u mogelijk het beste de DN-naam (Distinguished Name) van uw adreslijstarchief op het hoogste niveau gebruiken.

Gebruikersvraag

Specificeer de query-informatie die de Bomgar Box moet gebruiken bij het vinden van een LDAP als de gebruiker probeert in te loggen. In het veld **Gebruikersquery** kunt u een standaard LDAP-query invoeren (RFC 2254: Representatie van de tekenreeks voor LDAP-zoekfilters). U kunt de voor de query te gebruiken tekenreeks aanpassen aan de manier waarop uw gebruikers inloggen en aan de methode waarop gebruikersnamen worden geaccepteerd. Om binnen de tekenreeks de waarde te specificeren die voor de gebruikersnaam wordt gebruikt, kunt u die waarde vervangen door een *.

Vraag zoeken

De zoekvraag bepaalt hoe resultaten worden weergegeven als via groepsbeleidslijnen wordt gezocht. Hiermee worden de resultaten gefilterd zodat alleen bepaalde resultaten in de vervolgkeuzelijst om leden te kiezen worden weergegeven als leden aan een groepsbeleidslijn worden toegevoegd.

Objectklassen

Specificeer geldige objectklassen voor een gebruiker binnen uw adreslijstarchief. Alleen gebruikers die een of meer van deze objectklassen bezitten, mogen verifiëren. Deze objectklassen worden ook met de onderstaande attribuutnamen gebruikt om aan uw Bomgar Box het schema aan te geven dat de LDAP-server gebruikt om gebruikers te identificeren. U kunt meerdere gebruikersobjectklassen invoeren, één per regel.

Attribuutnamen

Specificeer welke velden moeten worden gebruikt als de unieke ID en schermnaam van een gebruiker.

Unieke id

In dit veld moet een unieke identificator voor het object worden ingevoerd. Hoewel de distinguised name (DN-naam) als deze identificator kan dienen, kan de distinguised name van een gebruiker gedurende de levensduur van de gebruiker vaak wijzigen, bijvoorbeeld bij een wijziging van de naam of van de locatie of als de naam van het LDAP-archief wordt gewijzigd. De meeste LDAP-servers beschikken daarom over een veld dat per object uniek is en gedurende de levensduur van de gebruiker niet wijzigt. Als u toch de distinguised name als de unieke identificator gebruikt en de distinguised name van een gebruiker wijzigt, dan wordt die gebruiker als een nieuwe gebruiker beschouwd en worden eventuele wijzigingen specifiek voor het Bomgar gebruikersaccount van die persoon niet naar de nieuwe gebruiker overgedragen. Als uw LDAP-server niet over een unieke identificator beschikt, dan kunt u een veld gebruiken waarvan de kans zo klein mogelijk is dat de waarde hiervan voor een andere gebruiker identiek is.

Gebruik hetzelfde attribuut voor publieke en privéschermnamen

Als deze optie is aangevinkt, dan kunt u aparte waarden specificeren voor de privé- en publieke schermnamen van de gebruiker.

Schermnamen

Met deze waarde wordt bepaald welke velden gebruikt moeten worden als de privé- en publieke schermnamen van de gebruiker.

Instellingen groepsschema *(Alleen zichtbaar tijdens het opzoeken van groepen)*

Basis DN opzoeken

Bepaal het niveau in uw adreslijst-hiërarchie, gespecificeerd door een DN-naam (Distinguished Name), waar de Bomgar Box moet beginnen naar groepen te zoeken. Afhankelijk van de grootte van uw adreslijstarchief en de groepen die toegang tot de Bomgar Box nodig hebben, kunt u de prestaties verbeteren door de specifieke organisatorische eenheid in uw adreslijstarchief aan te wijzen waar toegang toe nodig is. Als u niet zeker weet of groepen binnen meerdere organisatorische eenheden actief zijn, kunt u mogelijk het beste de DN-naam (Distinguished Name) van uw adreslijstarchief op het hoogste niveau gebruiken.

Vraag zoeken

De zoekvraag bepaalt hoe resultaten worden weergegeven als via groepsbeleidslijnen wordt gezocht. Hiermee worden de resultaten gefilterd zodat alleen bepaalde resultaten in de vervolgkeuzelijst om leden te kiezen worden weergegeven als leden aan een groepsbeleidslijn worden toegevoegd.

Objectklassen

Specificeer geldige objectklassen voor een groep binnen uw map-archieven. Alleen groepen die een of meer van deze objectklassen bezitten, worden geretourneerd. Deze objectklassen worden ook met de onderstaande attribuutnamen gebruikt om aan uw Bomgar Box het schema aan te geven dat de LDAP-server gebruikt om groepen te identificeren. U kunt meerdere groepsobjectklassen invoeren, op elke regel één.

Attribuutnamen

Specificeer welke velden moeten worden gebruikt als de unieke ID en schermnaam van een groep.

Unieke id

In dit veld moet een unieke identificator voor het object worden ingevoerd. Hoewel de onderscheiden naam als deze identificator kan dienen, kan de onderscheiden naam van een groep gedurende de levensduur van een groep vaak wijzigen, bijvoorbeeld bij

een locatiewijziging of als de naam van het LDAP-archief wordt gewijzigd. De meeste LDAP-servers beschikken daarom over een veld dat per object uniek is en gedurende de levensduur van de groep niet wijzigt. Als u toch de onderscheiden naam als de unieke identificator gebruikt en de onderscheiden naam van een groep wijzigt, dan wordt die groep als een nieuwe groep beschouwd en worden eventuele voor die groep gedefinieerde groepsbeleidslijnen niet naar de nieuwe groep overgedragen. Als uw LDAP-server niet over een unieke identificator beschikt, dan kunt u een veld gebruiken waarvan de kans zo klein mogelijk is dat de waarde hiervan voor een andere groep identiek is.

Schermnaam

Deze waarde bepaalt welk veld moet worden gebruikt als de schermnaam van de groep.

Relaties tussen gebruikers en groepen

U moet in dit veld een vraag invoeren om te bepalen welke gebruikers tot welke groepen behoren of, andersom, welke groepen welke gebruikers bevatten.

Recursieve zoekopdracht uitvoeren voor groepen

U kunt recursief naar groepen zoeken. Er wordt dan een zoekopdracht naar een gebruiker uitgevoerd, vervolgens zoekopdrachten voor alle groepen waar die gebruiker toe behoort enzovoort totdat alle mogelijke groepen die met die gebruiker geassocieerd zijn, zijn gevonden.

Het uitvoeren van een recursieve zoekopdracht kan een grote invloed op de prestaties hebben, omdat de server voortdurend zoekopdrachten uitzet tot alle informatie over alle groepen gevonden is. Als dit te lang duurt, dan kan de gebruiker mogelijk niet inloggen.

Bij niet-recursief zoeken wordt er per gebruiker maar één zoekopdracht uitgevoerd. Als uw LDAP-server over een speciaal veld beschikt met alle groepen waar de gebruiker toe behoort, dan is recursief zoeken niet nodig. Recursief zoeken is ook niet nodig als het ontwerp van uw mapstructuur geen groepsleden van groepen ondersteunt.

Instellingen testen

Gebruikersnaam en wachtwoord

Voer een gebruikersnaam en wachtwoord in voor een account dat op de door u te testen server bestaat. Dit account moet overeenkomen met de inlog-criteria die in bovenstaande configuratie zijn gespecificeerd.

Probeer de gebruikerskenmerken en groepslidmaatschappen te krijgen als de inloggegevens worden geaccepteerd

Als deze optie is aangevinkt en het testen van inloggegevens is geslaagd, dan wordt ook geprobeerd de gebruikersattributen te controleren en de groep op te zoeken. Let op: om de test van deze functies te laten slagen, moeten ze door uw beveiligingsprovider ondersteund worden en moeten ze daar geconfigureerd zijn.

Test starten

Als uw server juist is geconfigureerd en u voor de test een geldige gebruikersnaam en wachtwoord hebt ingevoerd, dan ontvangt u een bericht dat de test geslaagd is. Anders ziet u een foutmelding en een logboekvermelding waarmee u het probleem kunt onderzoeken.

Beveiligingsproviders :: Bewerken: RADIUS

Algemene instellingen

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

Ingeschakeld: Deze provider is ingeschakeld

Indien dit veld is aangevinkt, kan uw Bomgar Box naar deze beveiligingsprovider zoeken als een gebruiker probeert in te loggen. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Schermnamen: Houd de schermnaam gesynchroniseerd met het systeem op afstand

Met deze waarden wordt bepaald welke velden gebruikt moeten worden voor de privé- en publieke schermnamen van de gebruiker.

Autorisatie-instellingen

Alleen de volgende gebruikers toelaten

U kunt ervoor kiezen alleen toegang toe te staan tot bepaalde gebruikers op uw RADIUS-server. Voer de gebruikersnamen op aparte regels in. Nadat de gebruikersnamen zijn toegevoegd, zijn de gebruikers beschikbaar vanaf de dialoog **Beleidslid toevoegen** wanneer u op de pagina **/login > Gebruikers en beveiliging > Groepsbeleidslijnen** groepsbeleidslijnen bewerkt.

Als u dit veld leeg laat, dan worden alle gebruikers toegestaan die tegen uw RADIUS-server worden geverifieerd. Als u iedereen toestaat, dan moet u ook een standaard groepsbeleid specificeren.

LDAP-groep opzoeken

Als u wilt dat gebruikers op deze beveiligingsprovider op een aparte LDAP-server met hun groepen worden geassocieerd, dan moet u een of meerdere LDAP-groepservers kiezen die bij het opzoeken van de groep moeten worden gebruikt.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet een lid van tenminste één groepsbeleid zijn om op uw Bomgar Box te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login interface ofwel de toegangsconsole. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Instellingen voor verbinding

Hostnaam

Voer de hostnaam in van de server waar uw externe adreslijstarchief staat.

Poort

Specificeer de verificatiepoort voor uw RADIUS-server. Meestal is dit poort **1812**.

Verbindingsmethode

Als u een extern adreslijstarchief gebruikt in hetzelfde lokale netwerk als uw Bomgar Box, dan kunnen de twee systemen direct met elkaar communiceren. In dat geval hoeft u de optie **Proxy van apparaat via de verbindingsagent** niet aan te vinken en kunt u verder gaan.

Als de twee systemen niet direct met elkaar kunnen communiceren, bijvoorbeeld als uw externe adreslijstserver achter een firewall staat, dan moet u een verbindingsagent gebruiken. Als u de Win32 verbindingsagent downloadt, dan kunnen uw adreslijstserver en uw Bomgar Box met elkaar communiceren via een uitgaande met SSL versleutelde verbinding zonder firewallconfiguratie. De verbindingsagent kan ofwel direct naar de adreslijstserver worden gedownload, ofwel naar een aparte server op hetzelfde netwerk als uw adreslijstserver (aanbevolen).

In het bovenstaande geval moet u **Proxy van apparaat via de verbindingsagent** aanvinken. Maak een **Wachtwoord verbindingsagent** aan om tijdens de installatie van de verbindingsagent te gebruiken. Klik vervolgens op **Verbindingsagent downloaden**, voer het installatieprogramma uit en volg de instructies van de installatiewizard op. Tijdens installatie wordt u gevraagd om de naam van de beveiligingsprovider in te voeren evenals het hier hierboven aangemaakte wachtwoord voor de verbindingsagent.

Gedeeld geheim

Geef een nieuw gedeeld geheim op om uw Bomgar Box en uw RADIUS-server met elkaar te laten communiceren.

Time-out (seconden)

Stel in hoe lang op antwoord van de server moet worden gewacht. Denk eraan dat als het antwoord **Antwoord-accepteren** of **Antwoord-uitdaging** is, dan wacht RADIUS gedurende de totale hier gedefinieerde tijd voordat het account wordt geverifieerd. Aanbevolen wordt daarom om deze waarde zo laag mogelijk in te stellen als uw netwerkinstellingen toestaan. De beste waarde is 3-5 seconden, de maximale waarde is drie minuten.

Instellingen voor cluster *(Alleen zichtbaar voor clusters)*

Selectie-algoritme voor leden

Selecteer de methode waarmee in deze cluster naar nodes wordt gezocht.

Bij **Van boven naar beneden** wordt eerst op de server met de hoogste prioriteit gezocht. Als die server niet beschikbaar is of als het account niet is gevonden, dan wordt op de server met de daarop volgende prioriteit gezocht. Vervolgens wordt in volgorde van aflopende prioriteit op de servers uit de lijst geclusterde servers gezocht tot het account is gevonden of blijkt dat het account niet op een van de gespecificeerde en beschikbare servers bestaat.

Round-robin is bedoeld om de belasting van de verschillende servers in balans te houden. Bij dit algoritme wordt de eerste server waarop wordt gezocht willekeurig gekozen. Als die server niet beschikbaar is of als het account niet is gevonden, dan wordt op een willekeurige andere server gezocht. Vervolgens wordt in willekeurige volgorde op de overige servers uit de lijst geclusterde servers gezocht tot het account is gevonden of blijkt dat het account niet op een van de gespecificeerde en beschikbare servers bestaat.

Wachttijd voor opnieuw proberen

Stel in hoe lang moet worden gewacht nadat een lid van een cluster niet beschikbaar is geworden voordat een nieuwe poging wordt gedaan voor dat lid van die cluster.

Instellingen testen

Gebruikersnaam en wachtwoord

Voer een gebruikersnaam en wachtwoord in voor een account dat op de door u te testen server bestaat. Dit account moet overeenkomen met de inlog-criteria die in bovenstaande configuratie zijn gespecificeerd.

Probeer de gebruikerskenmerken en groepslidmaatschappen te krijgen als de inloggegevens worden geaccepteerd

Als deze optie is aangevinkt en het testen van inloggegevens is geslaagd, dan wordt ook geprobeerd de gebruikersattributen te controleren en de groep op te zoeken. Let op: om de test van deze functies te laten slagen, moeten ze door uw beveiligingsprovider ondersteund worden en moeten ze daar geconfigureerd zijn.

Test starten

Als uw server juist is geconfigureerd en u voor de test een geldige gebruikersnaam en wachtwoord hebt ingevoerd, dan ontvangt u een bericht dat de test geslaagd is. Anders ziet u een foutmelding en een logboekvermelding waarmee u het probleem kunt onderzoeken.

Beveiligingsproviders :: Bewerken: Kerberos

Algemene instellingen

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

Ingeschakeld: Deze provider is ingeschakeld

Indien dit veld is aangevinkt, kan uw Bomgar Box naar deze beveiligingsprovider zoeken als een gebruiker probeert in te loggen. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Gebruikers- en schermnamen: Houd de schermnaam gesynchroniseerd met het systeem op afstand

Met deze waarden wordt bepaald welke velden gebruikt moeten worden voor de privé- en publieke schermnamen van de gebruiker.

Realm verwijderen uit principal-namen

Selecteer deze optie om bij het samenstellen van de Bomgar gebruikersnaam het REALM-gedeelte van de Principal-naam van gebruiker te verwijderen.

Autorisatie-instellingen

Gebruikersafhandelingsmodus

Selecteer welke gebruikers op uw Bomgar Box kunnen worden geverifieerd. Met **Alle gebruikers toelaten** wordt iedereen toegelaten die momenteel via uw KDC wordt geverifieerd. Met **Alleen gebruikers-principals toelaten die op de lijst zijn gespecificeerd** worden alleen gebruikers-principals toegelaten die expliciet zijn vermeld. Met **Alleen gebruikers-principals toelaten die met de regex overeenkomen** worden alleen gebruikers-principals toegelaten die met een Perl-compatibele reguliere expressie (PCRE) overeenkomen.

SPN-afhandelingsmodus: Laat alleen SPN's toe die op de lijst zijn gespecificeerd

Als dit veld niet is aangevinkt, dan worden alle service-principal-namen (SPN's) voor deze beveiligingsprovider toegelaten. Als dit veld is aangevinkt, dan moet u specifieke SPN's uit een lijst van momenteel geconfigureerde SPN's selecteren.

LDAP-groep opzoeken

Als u wilt dat gebruikers op deze beveiligingsprovider op een aparte LDAP-server met hun groepen worden geassocieerd, dan moet u een of meerdere LDAP-groepservers kiezen die bij het opzoeken van de groep moeten worden gebruikt.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet een lid van tenminste één groepsbeleid zijn om op uw Bomgar Box te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login interface ofwel de toegangsconsole. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Sessiebeleidslijnen: Sessiemachtigingen en prompt-regels instellen

Sessiebeleidslijnen

Met sessiebeleidslijnen kunt u sessiebeveiligingsmachtigingen aan specifieke scenario's aanpassen. Sessiebeleidslijnen kunnen op gebruikers en Jump-clients worden toegepast.

In de sectie **Sessiebeleidslijnen** staat een lijst met beschikbare beleidslijnen. Klik op het pijltje naast een beleidsnaam om snel te zien waar dat beleid wordt gebruikt, of het voor gebruikers, toegangsuitnodigingen en Jump-clients beschikbaar is en welke hulpmiddelen zijn geconfigureerd.

Nieuw beleid aanmaken, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Kopiëren

Om het aanmaken van gelijksoortige beleidslijnen te versnellen, kunt u op **Kopiëren** klikken om een nieuwe beleidslijn aan te maken met identieke instellingen. U kunt deze nieuwe beleidslijn dan bewerken om aan uw wensen te voldoen.

Sessiebeleid :: Toevoegen of bewerken

Beleidsinstellingen

Schermnaam

Maak een unieke naam aan om te helpen dit object te identificeren. Deze naam helpt bij het toekennen van een sessiebeleid aan gebruikers en Jump-clients.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, wordt er automatisch een aangemaakt.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit object samen te vatten. U kunt de beschrijving zien als u een beleid op gebruikersaccounts, groepsbeleidslijnen en toegangsuitnodigingen toepast.

Beschikbaarheid: Gebruikers

Kies of dit beleid beschikbaar moet zijn om aan gebruikers toe te wijzen (gebruikersaccounts en groepsbeleidslijnen).

Beschikbaarheid: Toegangsuitnodiging

Kies of dit beleid beschikbaar moet zijn om gebruikers te selecteren die worden uitgenodigd om een sessie bij te wonen.

Beschikbaarheid: Jump-clients

Kies of dit beleid beschikbaar moet zijn om aan Jump-clients toe te wijzen.

Beschikbaarheid: Afhankelijkheden

Als dit sessiebeleid al in gebruik is, dan ziet u het aantal gebruikers en Jump-clients dat dit beleid gebruikt.

Gereedschappen

U kunt voor alle volgende machtigingen ervoor kiezen deze te activeren of uit te schakelen of u kunt ervoor kiezen deze op **Niet gedefinieerd** in te stellen. Sessiebeleidslijnen worden hiërarchisch op een sessie toegepast, waarbij Jump-clients de hoogste prioriteit krijgen, dan gebruikers en dan de algemene standaard. Als er meerdere beleidslijnen op een sessie van toepassing zijn, dan krijgt het beleid met de hoogste prioriteit voorrang boven het andere. Als het op een Jump-client toegepaste beleid bijvoorbeeld een machtiging definieert, dan mogen gedurende de sessie geen andere beleidslijnen die machtiging wijzigen. Om ervoor te zorgen dat een machtiging door een beleid op een lager niveau kan worden gedefinieerd, dan moet die machtiging op **Niet gedefinieerd** zijn ingesteld. Zie Gebruik van sessiebeleidslijnen voor meer informatie en voorbeelden.

Stel in welke hulpmiddelen met dit beleid moeten worden in- of uitgeschakeld.

Scherm delen

Hierdoor kan de gebruiker het externe scherm bekijken of besturen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.

> ***Opmerking:*** *Deze functie geldt alleen voor Windows en Linux besturingssystemen en geldt niet voor sessies met bureaublad op afstand (RDP).*

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar één of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Opmerking: *Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.*

Toegestane eindpuntbeperkingen

Stel in of de gebruiker de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.

Mag inloggen met inloggegevens van een beheerder van verificatiegegevens voor een eindpunt

Activeer een verbinding van een gebruiker naar de beheerder van eindpunt-verificatiegegevens vanaf uw bestaande wachtwoord-opslagplaatsen of -kluizen.

Voor gebruik van Beheerder van verificatiegegevens voor eindpunt is een aparte onderhoudsovereenkomst met Bomgar vereist. Als een onderhoudsovereenkomst eenmaal is afgesloten, mag u de benodigde middleware vanuit het Bomgar self-service center downloaden.

Opmerking: *In eerdere versies dan 15.2 is deze functie alleen beschikbaar in sessies die vanaf een opgewaardeerde Jump-client op Windows® zijn gestart. Vanaf versie 15.2 mag u ook een beheerder van eindpunt-verificatiegegevens gebruiken in sessies met externe Jump, met Microsoft® bureaublad op afstand of met Shell Jump. U kunt deze functie ook gebruiken in een sessie met scherm delen op een Windows® systeem door gebruik te maken van de speciale actie Uitvoeren als.*

Annotaties

Hierdoor kan de gebruiker gereedschappen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.

Opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer zien. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toestemming tot gebruik van systeeminformatie-acties

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

Register-toegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

Standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Opwaardering

Hierdoor kan de gebruiker proberen de eindpunt-client op te waarderen zodat deze met beheerdersrechten op het externe systeem kan worden uitgevoerd. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Beleid opslaan

Klik op **Beleid opslaan** om dit beleid beschikbaar te stellen.

Beleid exporteren

U kunt een sessiebeleid van de ene site exporteren en die machtigingen naar een beleid op een andere site importeren. Bewerk het beleid dat u wilt exporteren en ga naar de onderkant van de pagina. Klik op **Beleid exporteren** en sla het bestand op.

Beleid importeren

U kunt die beleidsinstellingen op een andere Bomgar site importeren die het importeren van sessiebeleid ondersteunt. Maak een nieuw sessiebeleid aan en ga naar de onderkant van de pagina. Blader naar het beleidsbestand en klik vervolgens op **Beleid importeren**. Nadat het beleidsbestand is geüpload wordt de pagina vernieuwd waarna u wijzigingen kunt aanbrengen. Klik op **Beleid opslaan** om het beleid beschikbaar te stellen.

Sessiebeleid-simulator

Omdat het gebruik van gelaagd beleid ingewikkeld kan zijn, kunt u de **Sessiebeleid-simulator** gebruiken om te bepalen wat het resultaat is. Bovendien kunt u de simulator gebruiken om te onderzoeken waarom een machtiging niet beschikbaar is als u het tegendeel verwacht.

Gebruiker

Selecteer eerst de gebruiker die de sessie uitvoert. Deze vervolgkeuzelijst bevat zowel gebruikersaccounts als uitnodigingsbeleidslijnen.

Sessiestartmethode

Selecteer de sessiestartmethode. Dit kan een **Jump-client**, een **Externe Jump** of een **Lokale Jump** zijn.

Jump-client/jumpsnelkoppeling

Zoek een jumpsnelkoppeling op naam, opmerkingen, Jumpgroep of tag.

Simuleren

Klik op **Simuleren**. In het gebied hieronder worden de machtigingen die door sessiebeleid kunnen worden geconfigureerd, in de modus alleen-lezen weergegeven. U kunt zien welke machtigingen wel en niet zijn toegestaan als resultaat van gestapelde beleidslijnen en door welke beleidslijn elk van de machtigingen is ingesteld.

Groepsbeleidslijnen: Gebruikersmachtigingen op groepen gebruikers toepassen

Groepsbeleidslijnen

Op de pagina **Groepsbeleidslijnen** kunt u groepen gebruikers instellen die dezelfde rechten delen.

Nieuw beleid aanmaken, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Kopiëren

Om het aanmaken van gelijksoortige beleidslijnen te versnellen, kunt u op **Kopiëren** klikken om een nieuwe beleidslijn aan te maken met identieke instellingen. U kunt deze nieuwe beleidslijn dan bewerken om aan uw wensen te voldoen.

Volgorde veranderen

Klik op deze knop om groepsbeleidslijnen te slepen en neer te zetten om de prioriteiten ervan in te stellen. Klik op **Volgorde opslaan** om de wijzigingen in de prioriteiten te effectueren. Voor beheerdoeleinden is de aanbevolen prioriteitsvolgorde om beleidslijnen te definiëren voor meer specifieke gebruikersgroepen als een hogere prioriteit (zodat deze niet kunnen worden overschreven) en vandaar naar lagere prioriteiten te werken en bredere groepen als een lagere prioriteit in te stellen.

Groepsbeleid :: Toevoegen of bewerken

Basisinstellingen

Inlogcode voor e-mail

Hierdoor wordt meervoudige verificatie toegestaan. Gebruikers ontvangen telkens wanneer zij op de /loging beheerinterface op de toegangsconsole inloggen een e-mail met een unieke verificatiecode, zowel op een computer als op een mobiel apparaat. Als de code drie keer achtereen onjuist wordt ingevoerd, dan moeten de gebruikers hun inloggegevens opnieuw invoeren en een nieuwe e-mailcode invoeren.

Naam beleid

Maak een unieke naam aan om te helpen dit object te identificeren.

Beleidsleden

Als u nieuwe leden wilt toewijzen, moet u op de knop **Toevoegen** klikken om een keuzevak te openen. Selecteer gebruikers van uw lokale systeem of selecteer gebruikers of hele groepen van geconfigureerde beveiligingsproviders. Om gebruikers of groepen van uit een extern adreslijstarchief toe te voegen zoals LDAP, RADIUS of Kerberos, moet u eerst op de pagina **/login > Gebruikers en beveiliging > Beveiligingsproviders** de verbinding configureren. Als een poging een gebruiker van een geconfigureerde

beveiligingsprovider toe te voegen ongeldig is, dan verschijnt er hier en in de logboekregistratie een melding van een synchronisatiefout.

Accountinstellingen

Gedefinieerd in dit beleid

Selecteer voor elke instelling of die in dit beleid moet worden gedefinieerd of dat de instelling voor individuele gebruikers moet worden geconfigureerd. Als de instelling hier moet worden gedefinieerd, dan kunt u die machtiging niet voor een individuele gebruiker vanaf diens accountpagina wijzigen.

Als u een beleid hebt dat een machtiging definieert en u wilt dat geen enkel beleid die machtiging kan overschrijven, dan moet u selecteren dat dat beleid niet kan worden overschreven en moet het beleid een hogere prioriteit hebben dan andere beleidslijnen die ook die instelling definiëren.

Account vervalt op

Hierdoor vervalt het account na een bepaalde datum of vervalt het nooit.

Account uitgeschakeld

Hierdoor wordt het account uitgeschakeld zodat de gebruiker niet kan inloggen. Als een account wordt uitgeschakeld, wordt het NIET verwijderd.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Machtigingen

Beheerder

Hoerdoor krijgt de gebruiker volledige beheerdersrechten.

Mag wachtwoorden instellen

Hierdoor kan de gebruiker wachtwoorden instellen en accounts ontgrendelen voor lokale gebruikers die geen beheerder zijn.

Mag Jumpoints bewerken

Hierdoor mogen gebruikers Jumpoints aanmaken of bewerken. Deze optie heeft geen invloed op de mogelijkheid voor de gebruikers om via Jumpoints toegang tot externe computers te krijgen. Dat wordt via beleid op Jumpoint- of groepsniveau geconfigureerd.

Toestemmingen voor toegangssessierapportage: Mag rapporten van toegangssessies bekijken

Hierdoor kan de gebruiker rapporten maken over activiteiten tijdens toegangssessies, waarbij hij of zij alleen sessies kan bekijken waarvan hij of zij de primaire sessie-eigenaar was, alleen sessies waarbij een van zijn of haar teams het primaire team was, alleen sessies waarin een van zijn of haar teamleden de primaire sessie-eigenaar was of alle sessies.

Mag opnames van toegangssessies bekijken

Hierdoor kan een gebruiker opnames bekijken van sessies met scherm delen en van sessies met opdrachtshell.

Mag rapportage API gebruiken

Hierdoor kunnen de inloggegevens van de gebruiker worden gebruikt om via de API XML-rapporten op te halen.

Mag opdracht API gebruiken

Hierdoor kunnen de inloggegevens van de gebruiker worden gebruikt om via de API opdrachten te geven.

Mag teams bewerken

Hierdoor kunnen gebruikers teams aanmaken of bewerken.

Mag standaard scripts bewerken

Hierdoor kan de gebruiker standaard scripts aanmaken of bewerken die worden gebruikt in sessies met scherm delen of met opdrachtshell.

Mag aangepaste links bewerken

Hierdoor kan de gebruiker aanpasbare koppelingen aanmaken of bewerken.

Toegangsmachtigingen

Toegang

Toestemming voor toegang tot eindpunten

Hierdoor mag de gebruiker de toegangsconsole gebruiken om sessies uit te voeren. Als toegang tot een eindpunt is ingeschakeld, dan zijn er ook opties beschikbaar die betrekking hebben op toegang tot een eindpunt.

Sessiebeheer

Mag sessies delen met teams waarvan hij/zij geen deel uitmaakt

Hierdoor kan de gebruiker behalve zijn of haar teamleden ook een minder beperkte groep gebruikers uitnodigen om sessies te delen. Samen met de machtiging Uitgebreide beschikbaarheid vormt deze machtiging een uitbreiding van de mogelijkheden om sessies te delen.

Mag externe gebruikers uitnodigen

Hierdoor kan de gebruiker een gebruiker van een derde partij uitnodigen eenmalig aan een sessie deel te nemen.

Mag modus Uitgebreide beschikbaarheid inschakelen

Hierdoor kan de gebruiker e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen, ook als hij of zij niet op de toegangsconsole is ingelogd.

Mag de externe sleutel bewerken

Staat gebruikers toe om de externe sleutel te wijzigen vanaf het informatiedeelvenster van een sessie binnen de toegangsconsole.

Scherm delen van gebruiker tot gebruiker

Mag scherm tonen aan andere gebruikers

Hierdoor kan een gebruiker zijn of haar scherm delen met een andere gebruiker zonder dat de ontvanger aan een sessie hoeft aan te melden. Deze optie is zelfs beschikbaar als de gebruiker niet in een sessie is.

Mag besturing geven tijdens tonen van scherm aan andere gebruikers

Hierdoor kan de gebruiker tijdens scherm delen de besturing over muis en toetsenbord aan de gebruiker geven die zijn of haar scherm bekijkt.

Jump-technologie

Toegestane Jump-methodes: Mag sessies opstarten via Jump-clients die een van de volgende Jump-methodes gebruiken:

Hierdoor kan de gebruiker een Jump uitvoeren naar computers via **Jump-clients**, **Lokale Jump op het lokale netwerk**, **Externe Jump via een Jumpoint**, **Bureaublad op afstand via een Jumpoint** en/of **Shell Jump via een Jumpoint**.

Machtigingen voor jumpsnelkoppelingen: Mag sessies van alle jumpsnelkoppelingen binnen het systeem starten

Hierdoor mag de gebruiker een Jump uitvoeren naar externe computers in alle Jumpgroepen van het team.

Mag jumpsnelkoppelingen implementeren, verwijderen en wijzigen in de volgende Jumpgroepen:

Hierdoor kan de gebruiker sessies vastspelden, groepen instellen en commentaar aan jumpsnelkoppelingen toevoegen voor zijn of haar persoonlijke Jumpgroep, voor Jumpgroepen van een team en van teamleden of voor alle Jumpgroepen, inclusief de Jumpgroepen die aan teams zijn toegewezen waar de gebruiker niet toe behoort en aan de persoonlijke Jumpgroep van elke gebruiker.

Mag de met jumpsnelkoppelingen geassocieerde sessiebeleidslijnen wijzigen

Hierdoor kan de gebruiker het sessiebeleid instellen dat een jumpsnelkoppeling moet gebruiken. Het wijzigen van het sessiebeleid kan van invloed zijn op de machtigingen in de sessie.

Sessietoestemmingen

Stel de prompts en de machtigingsregels in die voor de sessies van deze gebruiker moeten gelden. Kies een bestaand sessiebeleid of definieer aangepaste machtigingen voor deze gebruiker. Als u **Niet gedefinieerd** specificeert, dan wordt het algemene standaard beleid gebruikt. Deze machtigingen kunnen door een beleid met hogere prioriteit worden overschreven.

Beschrijving

Bekijk de omschrijving van een vooraf gedefinieerd beleid voor sessietoestemming.

Scherm delen

Scherm delen

Hierdoor kan de gebruiker het externe scherm bekijken of besturen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.

> ***Opmerking:*** *Deze functie geldt alleen voor Windows en Linux besturingssystemen en geldt niet voor sessies met bureaublad op afstand (RDP).*

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar één of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Opmerking: *Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.*

Toegestane eindpuntbeperkingen

Stel in of de gebruiker de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.

Mag inloggen met inloggegevens van een beheerder van verificatiegegevens voor een eindpunt

Activeer een verbinding van een gebruiker naar de beheerder van eindpunt-verificatiegegevens vanaf uw bestaande wachtwoord-opslagplaatsen of -kluizen.

Voor gebruik van Beheerder van verificatiegegevens voor eindpunt is een aparte onderhoudsovereenkomst met Bomgar vereist. Als een onderhoudsovereenkomst eenmaal is afgesloten, mag u de benodigde middleware vanuit het Bomgar self-service center downloaden.

Opmerking: *In eerdere versies dan 15.2 is deze functie alleen beschikbaar in sessies die vanaf een opgewaardeerde Jump-client op Windows® zijn gestart. Vanaf versie 15.2 mag u ook een beheerder van eindpunt-verificatiegegevens gebruiken in sessies met externe Jump, met Microsoft® bureaublad op afstand of met Shell Jump. U kunt deze functie ook gebruiken in een sessie met scherm delen op een Windows® systeem door gebruik te maken van de speciale actie Uitvoeren als.*

Annotaties

Hierdoor kan de gebruiker gereedschappen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Bestandsoverdracht

Bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.

Opdrachtshell

Opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Systeeminformatie

Systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer zien. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toestemming tot gebruik van systeeminformatie-acties

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

Register-toegang

Register-toegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

Andere hulpprogramma's

Standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Opwaardering

Hierdoor kan de gebruiker proberen de eindpunt-client op te waarderen zodat deze met beheerdersrechten op het externe systeem kan worden uitgevoerd. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Inlogschema

Beperk inloggen van gebruiker aan de hand van het volgende rooster

Stel een rooster in om te definiëren wanneer gebruikers op de toegangsconsole in kunnen loggen. Stel de tijdzone in die u voor dit rooster wilt gebruiker en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als bijvoorbeeld de begintijd is ingesteld op 08:00 uur en de eindtijd op 17:00 uur, dan kan een gebruiker op elk tijdstip in deze periode inloggen en kan blijven doorwerken tot na de eindtijd. De gebruiker kan echter na 17:00 uur niet opnieuw inloggen.

Forceer uitloggen als het schema inloggen niet toestaat

Als strengere toegangscontrole is vereist, dan moet u deze optie aanvinken. Hierdoor wordt de gebruiker geforceerd op de geplande eindtijd uit te loggen. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd. Wanneer de gebruiker uitgelogd wordt, volgen eventuele eigen sessies de sessieterugval-regels.

Lidmaatschappen

Teams

Geeft de teams aan waar gebruikers in deze groep aan moeten worden toegevoegd. Als een gebruiker in een andere groep zit die gebruikers aan een team toevoegt, maar u niet wilt dat gebruikers in deze groep in dat team zitten, dan moet u dit beleid instellen om gebruikers uit dat team te verwijderen. Handmatig aan een team toegevoegde gebruikers kunnen niet via groepsbeleid worden verwijderd.

Jumpoints

Geeft Jumpoints aan waar gebruikers in deze groep toegang toe hebben.

Alleen bij groepsbeleidslijnen geldt dat als een gebruiker in een andere groep zit die toegang tot een Jumpoint geeft, maar u niet wilt dat gebruikers in deze groep toegang tot dat Jumpoint krijgen, dan moet u dit beleid instellen om gebruikers van dat Jumpoint te verwijderen. Handmatig aan een Jumpoint toegevoegde gebruikers kunnen niet via groepsbeleid worden verwijderd.

Beleid opslaan

Klik op **Beleid opslaan** om het beleid te effectueren.

Beleid exporteren

U kunt een groepsbeleid vanuit een site exporteren en die machtigingen naar een beleid op een andere site importeren. Bewerk het beleid dat u wilt exporteren en ga naar de onderkant van de pagina. Klik op **Beleid exporteren** en sla het bestand op.

Opmerking: *Als u een groepsbeleid exporteert worden alleen de beleidsnaam, accountinstellingen en machtigingen geëxporteerd. Beleidsleden, teamlidmaatschappen en Jumpoint-lidmaatschappen worden bij het exporteren niet meegenomen.*

Beleid importeren

U kunt geëxporteerde beleidsinstellingen naar een andere Bomgar site importeren die het importeren van groepsbeleid ondersteunt. Maak een nieuw groepsbeleid aan of bewerk een bestaand beleid waarvan u de machtigingen wilt overschrijven en ga naar de onderkant van de pagina. Blader naar het beleidsbestand en klik vervolgens op **Beleid importeren**. Nadat het beleidsbestand is geüpload wordt de pagina vernieuwd waarna u wijzigingen kunt aanbrengen. Klik op **Beleid opslaan** om het groepsbeleid te effectueren.

Opmerking: *Als u een beleidsbestand in een bestaand groepsbeleid importeert, dan worden eventuele eerder gedefinieerde machtigingen overschreven, met uitzondering van beleidsleden, teamlidmaatschappen en Jumpoint-lidmaatschappen.*

Kerberos Keytab: De Kerberos Keytab beheren

Kerberos Keytab Beheer

Bomgar ondersteunt de eenmalige aanmelding door middel van het Kerberos verificatieprotocol. Hiermee kunnen gebruikers op de Bomgar Box worden geverifieerd zonder hun inloggegevens in te hoeven voeren. Kerberos verificatie geldt zowel voor de /login webinterface als voor de toegangsconsole.

Om Kerberos met uw Bomgar Box te integreren moet u een Kerberos systeem al hebben geïmplementeerd of bezig zijn met de implementatie ervan. De vereisten zijn als volgt:

- U moet een werkend Key Distribution Center (KDC) hebben.
- De klokken moeten op alle apparaten, het KDC en de Bomgar Box gesynchroniseerd zijn. Met een Network Time Protocol-server (NTP) is dit eenvoudig te regelen.
- U moet op het KDC een Service Principal-naam (SPN) voor uw Bomgar Box hebben aangemaakt.

Geconfigureerde principals

De sectie **Geconfigureerde principals** bevat een overzicht van alle beschikbare SPN's voor elke keytab die u hebt geüpload.

Als u SPN's beschikbaar hebt, dan kunt u vanaf de pagina **Beveiligingsproviders** een Kerberos beveiligingsprovider configureren en definiëren welke gebruikers-principals via Kerberos voor de Bomgar Box mogen worden geverifieerd.

Keytab importeren

Uploaden

Exporteer de keytab voor de SPN vanaf uw KDC en upload deze via de sectie **Keytab importeren** op deze pagina naar de Bomgar Box.

Rapporten: Rapport over sessie-activiteit

Rapporten :: Toegang

Beheerders en bevoorrechte gebruikers kunnen brede, volledige rapporten genereren en ook specifieke filters toepassen om de informatie in de rapporten aan de specifieke behoefte aan te passen.

Rapporttype

Genereer activiteitenrapporten volgens drie aparte rapporttypen: **Sessie**, **Samenvatting** en **Forensische gegevens van sessies** (indien ingeschakeld).

Filters

Pas indien nodig filters toe om uit de drie basistypen rapporten meer aangepaste rapporten af te leiden. Schakel naar wens een of meer filters in, maar alleen sessies die aan alle geselecteerde filters voldoen, worden weergegeven.

Sessie-ID of volgnummer

Voor deze unieke identificator is vereist dat u de ID (LSID) of het volgnummer specificeert voor die ene sessie die u zoekt. Dit is vaak handig als u een extern ticketsysteem of CRM-integratie hebt . U kunt dit filter niet met andere combineren.

Datumbereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Eindpunt

Filter sessies op computernaam, publiek IP-adres of privé-IP-adres.

Gebruiker

Gebruik de vervolgkeuzelijst om het type gebruikersdeelname te kiezen dat u wilt bijvoegen. Kies sessies waar een bepaalde gebruiker aan deel heeft genomen of waar een gebruiker uit een team aan deel heeft genomen, inclusief sessies die nooit met het gespecificeerde team geassocieerd zijn geweest.

Externe code

Filter om rapporten te genereren voor sessies die dezelfde externe code hebben gebruikt.

Alleen voltooide sessies bijvoegen

Filter om alleen sessies bij te voegen die voltooid zijn. Sessies die nog actief zijn, worden niet bijgevoegd.

Rapport toegangssessie

Bekijk alle sessies die aan de op de vorige pagina gespecificeerde criteria voldoen. Sessierapporten bevatten basisinformatie over de sessie plus koppelingen naar sessiedetails, transcripties van chats en video-opnames van scherm delen en opdrachtshells.

Detail van toegangssessie

Sessierapporten bevatten een opname van de transcriptie van de volledige chat, het aantal overgedragen bestanden en bepaalde acties die tijdens de sessie zijn uitgevoerd. Gebeurtenissen in vensters die duidelijke visuele wijzigingen in een sessie voorstellen worden als gebeurtenissen in de sessiedetails opgenomen. Dit betreft hoofdzakelijk veranderingen in het voorgrondvenster, met de naam van het uitvoerbare programma en de schermtitel.

Andere sessie-informatie betreft de duur van de sessie, lokale en externe IP-adressen en informatie over het externe systeem (indien ingeschakeld). Rapporten kunnen online worden bekeken of naar uw lokale systeem worden gedownload.

Als sessie-opname is ingeschakeld, dan kunt u video-opnames van individuele sessies bekijken, inclusief bijschriften van wie op een bepaald punt in de sessie de besturing van de muis en het toetsenbord had. Als het opnemen van de opdrachtregel is ingeschakeld, dan kunt u ook de opnames en/of transcripties van de tekst zien voor alle opdrachtshells die tijdens de sessie zijn uitgevoerd. Alle opnames worden op de Bomgar Box in ruwe opmaak opgeslagen en worden naar gecomprimeerde opmaak geconverteerd om te bekijken of te downloaden.

Samenvattingsrapport openen

Er zijn rapporten met samenvattingen van de activiteiten in de loop der tijd, gecategoriseerd per gebruiker. Er zijn statistieken voor het totaal aantal uitgevoerde sessies, het gemiddeld aantal sessies per weekdag en de gemiddelde duur van de sessies.

Rapporten :: Teamactiviteit

Start, duur en einde van een bereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Beperk tot

Kies het team waarvoor u de activiteitenlogboeken wilt bekijken.

Rapport teamactiviteit

Bekijk alle teamactiviteit die aan de op de vorige pagina gespecificeerde criteria voldoet. Rapporten over teamactiviteit bevatten informatie over de gebruikers wanneer die op de toegangsconsole in- of uitloggen, chatberichten tussen teamleden, acties voor scherm delen tussen gebruikers onderling die in de chat zijn gelogd en gedeelde en gedownloade bestanden.

Beheer

Softwarebeheer: Een back-up downloaden, software bijwerken

Software :: Instellingen voor back-up

Het is een belangrijke goede gewoonte voor herstel na rampen om regelmatig een back-upkopie van uw software-instellingen te maken. Bomgar beveelt aan om elke keer wanneer de configuratie van uw Bomgar Box wijzigt, een back-up van die configuratie te maken. In het geval van een hardwarestoring kunt u met een back-upbestand het herstel versnellen en, indien nodig, van Bomgar toegang krijgen tot tijdelijke services met behoud van de instellingen van uw laatste back-up.

Backup wachtwoord

Maak een wachtwoord aan om uw software-back-upbestand met een wachtwoord te beveiligen. Als u ervoor kiest een wachtwoord in te stellen, dan hebt u alleen toegang tot de back-up als u het wachtwoord invoert.

Inclusief logboekgegevens geschiedenis

Als deze optie is aangevinkt, dan bevat uw back-up logboekregistraties van sessies. Als deze optie niet is aangevinkt, dan staan er in uw back-up geen rapportage-gegevens voor sessies.

Backup downloaden

Bewaar een beveiligde kopie van uw softwareconfiguratie. Bewaar dit bestand op een veilige plaats.

Software :: Instellingen herstellen

Backupbestand

Als u een back-up moet herstellen, ga dan naar het allerlaatste back-upbestand dat u hebt bewaard.

Backup wachtwoord

Als u een wachtwoord voor uw back-upbestand hebt aangemaakt, voer dat dan hier in.

Backup uploaden

Upload het back-upbestand naar uw Bomgar Box en herstel de instellingen van uw site met de instellingen van de back-up.

Software :: Update uploaden

Gebruik **Software-update uploaden** om handmatig nieuwe softwarepakketten van Bomgar te uploaden. U wordt gevraagd te bevestigen dat u het softwarepakket wilt uploaden. In de sectie **Update geüpload** wordt extra informatie weergegeven waarmee u uw geüploade pakket kunt verifiëren. Klik op **Installeren** als u de installatie wilt voltooien of op **Update verwijderen** als u de update van de tijdelijke locatie wilt verwijderen. Als uw updatepakket alleen extra licenties bevat, dan kunt u de update installeren zonder het apparaat opnieuw te starten. Nadat u hebt bevestigd dat u wilt installeren verschijnt op de pagina een voortgangsbalk om u over het algehele installatieproces te informeren. Hier gemaakte updates werken automatisch alle sites en licenties op uw Bomgar Box bij.

Opmerking: *De beheerder van uw Bomgar Box kan ook de functie* ***Controleren op updates*** *in de /appliance interface gebruiken om automatisch naar nieuwe softwarepakketten te zoeken en deze te installeren.*

Beveiliging: Beveiligingsinstellingen beheren

Beveiliging :: Opties

Minimumlengte wachtwoord

Stel regels in voor lokale gebruikersaccounts voor de lengte van wachtwoorden.

Complexe wachtwoorden vereist

Stel regels in voor lokale gebruikersaccounts voor de complexiteit van wachtwoorden.

Standaard wachtwoordverloop

Stel regels in voor lokale gebruikersaccounts voor hoe vaak wachtwoorden verlopen.

Wachtwoord resetten inschakelen

Stel regels in voor lokale gebruikersaccounts of een vergeten wachtwoord kan worden gereset na een beveiligingsvraag juist te hebben beantwoord.

Opgeslagen logins activeren

Sta al dan niet toe of de toegangsconsole de inloggegevens van een gebruiker mag onthouden.

Accountvergrendeling na

Stel het aantal keren in dat een onjuist wachtwoord mag worden ingevoerd voordat het account wordt vergrendeld.

Sessie beëindigen als account wordt gebruikt

Als een gebruiker probeert op de toegangsconsole in te loggen met een account dat al in gebruik is, dan wordt, als het keuzevakje **Sessie beëindigen** is aangevinkt, de vorige verbinding verbroken zodat de gebruiker op de nieuwe verbinding mag inloggen.

Klembordsynchronisatiemodus

Met **Klembordsynchronisatiemodus** wordt bepaald hoe gebruikers binnen een sessie met scherm delen klemborden mogen synchroniseren. De beschikbare instellingen zijn als volgt:

- **Niet toegestaan**: de gebruiker heeft geen toegang tot het klembord op de externe computer en mag dit niet wijzigen.
- **Klembord handmatig verzenden van ondersteuningstechnicus naar klant toegestaan**: de gebruiker kan op een knop klikken om de inhoud van het lokale klembord naar het klembord op de externe computer te kopiëren.
- **Klembord handmatig verzenden in beide richtingen toegestaan**: de gebruiker kan op een knop klikken om de inhoud van het lokale klembord naar het klembord op de externe computer te kopiëren of om de inhoud van het klembord op de externe computer naar zijn of haar lokale klembord te kopiëren.

- **Automatische verzending van wijzigingen in klembord in beide richtingen**: de inhoud van het lokale en externe klembord blijven automatisch gesynchroniseerd.

U MOET de software opnieuw starten op de statuspagina om deze instellingen door te voeren.

Validatie SSL-certificaat

Als de certificaatketen niet kan worden gevalideerd, dan wordt de verbinding niet toegestaan.

Als certificaatvalidatie is uitgeschakeld en vervolgens wordt ingeschakeld, dan worden alle consoles en clients automatisch bijgewerkt wanneer zij de volgende keer verbinding maken. NB: LDAP-verbindingsagenten worden niet automatisch bijgewerkt maar moeten opnieuw worden geïnstalleerd om deze instelling te effectueren.

Als **Validatie SSL-certificaat** is ingeschakeld, dan worden extra beveiligingscontroles naast de in Bomgar ingebouwde beveiliging uitgevoerd om de SSL-certificaatketen te valideren die voor beveiligde communicatie gebruikt wordt. U wordt dringend aanbevolen SSL-validatie in te schakelen. Als certificaatvalidatie is uitgeschakeld, dan verschijnt in uw beheerinterface een waarschuwing. U kunt deze waarschuwing dertig dagen lang verbergen.

> ***Opmerking:*** *Om SSL-certificaatvalidatie in te schakelen moet u uw SSL-certificaat aan Bomgar zenden zodat het certificaat in uw Bomgar software kan worden opgenomen.*

Dagen voor het behouden van inlog-informatie

In **Dagen voor het behouden van inlog-informatie** kunt u instellen hoe lang inlog-informatie in de Bomgar Box moet worden opgeslagen. Deze informatie bestaat uit de rapportagegegevens en opnames van sessies.

Vooraf gedeelde sleutel (code) voor communicatie tussen apparaten

Voer in het veld **Vooraf gedeelde sleutel voor communicatie tussen Bomgar Boxen** een wachtwoord in om een vertrouwde relatie tussen twee Bomgar Boxen te maken. Als twee of meer Bomgar Boxen worden geconfigureerd voor functies als automatische omschakeling of clusteren, dan moeten de sleutels overeenstemmen. De sleutel moet uit tenminste 6 tekens bestaan en moet minstens één hoofdletter, één kleine letter, één cijfer en één speciaal teken bevatten.

Beveiliging :: Netwerkbeperkingen

Bepaal welke IP-netwerken toegang tot /login en /api op uw Bomgar Box moeten kunnen krijgen.

Sta toe vanaf alle netwerken

Er zijn geen netwerkbeperkingen van kracht.

Alleen de volgende netwerken toelaten

Er kan alleen vanaf de IP-adressen in de lijst toegang tot uw Bomgar Box op /login of /api worden verkregen.

Alleen de volgende netwerken weigeren

Er kan vanaf alle IP-adressen, behalve vanaf die in de lijst, toegang tot uw Bomgar Box op /login of /api worden verkregen.

Als u **Alleen tijdens de eerste verificatie van de gebruiker** selecteert, dan moet een gebruiker de eerste keer dat hij of zij op de toegangsconsole inlogt, zich op een toegestaan netwerk bevinden. Op dat moment wordt een token naar het apparaat gezonden zodat een volgende keer vanaf elke netwerklocatie op de toegangsconsole kan worden ingelogd.

Als u **Altijd** selecteert, dan moet een gebruiker altijd als hij of zij op de toegangsconsole inlogt, zich op een toegestaan netwerk bevinden.

Als u **Nooit** selecteert, dan kan een gebruiker vanaf elke netwerklocatie op de toegangsconsole inloggen.

Beveiliging :: Poortbeperkingen voor Administratieve-webinterface

Stel de poorten in waarvandaan toegang tot uw /login interface kan worden verkregen.

Websiteconfiguratie: HTTP-poorten instellen, vereiste inlogovereenkomst inschakelen

Site :: HTTP

HTTP-poort en HTTPS-poort

Ervaren netwerkspecialisten kunnen in een niet-standaard netwerk de poorten wijzigen waar het Bomgar verkeer langs gaat. Deze poort-instellingen mogen alleen worden aangepast wanneer andere dan de standaard poorten 80 en 443 voor webtoegang worden gebruikt.

Site :: /login Vereiste inlogovereenkomst

Inlogovereenkomst activeren

U kunt een inlogovereenkomst activeren die gebruikers moeten accepteren voordat zij toegang krijgen tot de /login beheerinterface. Met de overeenkomst, die u aan kunt passen, kunt u beperkingen en interne beleidsregels specificeren voordat gebruikers mogen inloggen.

Titel overeenkomst

Pas de titel van de overeenkomst aan.

Tekst overeenkomst

Geef de tekst voor de inlogovereenkomst.

E-mailconfiguratie: Software configureren om e-mails te verzenden

Configuratie :: E-mailadres

Opmerking: *Als een apparaat is aangewezen als een back-up-apparaat of een verkeers-node, dan wordt de e-mailconfiguratie voor dat apparaat overschreven met de e-mailconfiguratie die op het primaire hoofdapparaat is gedefinieerd.*

Van adres

Stel het e-mailadres in waarvandaan automatische berichten vanaf uw Bomgar Box worden verzonden.

Configuratie :: SMTP-relayserver

Configureer uw Bomgar Box om met uw SMTP-relayserver samen te werken om per e-mail automatisch kennisgevingen over bepaalde gebeurtenissen te verzenden.

SMTP-relayserver

Voer de hostnaam of het IP-adres van uw SMTP-relayserver in.

SMTP-poort

Stel de SMTP-poort voor contact met deze server in.

SMTP-encryptie

Als uw SMTP-server SSL-encryptie ondersteunt, kies dan **SSL** of **TLS**. Selecteer anders **Geen**.

SMTP-gebruikersnaam

Als uw SMTP-server verificatie vereist, voert u een gebruikersnaam in.

SMTP-wachtwoord

Als uw SMTP-server verificatie vereist, voert u een wachtwoord in.

Configuratie :: Contactpersoon Admin

Standaard Contactpersoon Admin e-mailadressen

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden.

Een test-e-mail verzenden als de instellingen zijn opgeslagen

Als u direct een test-e-mail wilt ontvangen om te verifiëren of uw SMTP-instellingen juist zijn geconfigureerd, vink dan deze optie aan voordat u op de knop **Veranderingen opslaan** klikt.

Verzenden dagelijkse communicatiekennisgeving

U kunt de Bomgar Box elke dag een kennisgeving laten verzenden om te controleren of de communicatie van waarschuwingen juist functioneert.

Naast de test-e-mail en de dagelijkse kennisgevingen die u hierboven kunt configureren, worden e-mails verzonden bij de volgende gebeurtenissen:

- Wanneer tijdens een automatische omschakeling de productversie op de primaire node niet overeenkomt met de productversie op de back-up-node.
- Wanneer tijdens een controle van de status van automatische omschakeling een van de volgende problemen wordt gedetecteerd.
    - Het huidige apparaat is de primaire node en in /login is een gedeeld IP-adres geconfigureerd, maar de netwerk-interface ervan is niet ingeschakeld.
    - In /login is een gedeeld IP-adres geconfigureerd, maar dit is in /appliance niet als een IP-adres opgenomen.
    - De back-up-node kon geen contact met de primaire node krijgen en evenmin met de test-IP-adressen die op de pagina **Beheer > Automatische omschakeling** zijn geconfigureerd.
    - De back-up-node kon geen contact met de test-IP-adressen krijgen die op de pagina **Beheer > Automatische omschakeling** zijn geconfigureerd.
    - De back-up-verwerking van de back-up-node is op de pagina **Beheer > Automatische omschakeling** uitgeschakeld.
    - De zelftest van de back-up-node is onverwacht mislukt, wat aangeeft dat het apparaat niet goed functioneert.
    - De back-up-node kon via de hostnaam van de primaire node geen contact met de primaire node krijgen.
    - Automatische omschakeling is uitgeschakeld en de back-up-node kon de primaire node niet testen.
    - Automatische omschakeling is ingeschakeld en de back-up-node kon de primaire node niet testen. De back-up-node wordt automatisch de primaire node als de primaire node geen antwoord meer geeft.
    - Automatische omschakeling is ingeschakeld en de back-up-node wordt automatisch de primaire node omdat de primaire node te lang offline was.
    - Gegevenssynchronisatie van de primaire node naar de back-up-node is op enig moment in de afgelopen 24 uur mislukt.

Uitgaande gebeurtenissen: Gebeurtenissen instellen om berichten uit te laten gaan

Uitgaande gebeurtenissen :: HTTP-geadresseerden

U kunt uw Bomgar Box configureren om berichten naar een HTTP-server of naar een e-mailadres te verzenden als verschillende gebeurtenissen optreden.

De door de Bomgar Box verzonden variabelen komen aan als een HTTP POST-methode en kunnen worden benaderd door de aanroepmethode die in uw coderingstaal wordt gebruikt om POST-gegevens op te halen. Als de server niet antwoordt met een HTTP 200 om aan te geven dat de overdracht is geslaagd, dan zet de Bomgar Box de huidige gebeurtenis opnieuw in de wachtrij en probeert later opnieuw het bericht te verzenden.

Nieuwe HTTP-geadresseerde toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Uitgaande gebeurtenissen :: HTTP-geadresseerde toevoegen of bewerken

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

URL

Voer de bestemmings-URL in voor de uitgaande gebeurtenis-handler .

Uitgeschakeld

Gebruik het selectievakje **Uitgeschakeld** om snel berichten te stoppen voor de gebeurtenis-handler die u instelt, bijvoorbeeld wanneer u een geplande integratietest uitvoert.

CA-certificaat

Als u via een HTTPS-verbinding werkt, dan moet u het basiscertificaat van de certificaatautoriteit uploaden dat door de uitgaande eventserver wordt geadverteerd.

Te verzenden gebeurtenissen

Kies welke gebeurtenissen berichten genereren die verzonden moeten worden.

Interval voor opnieuw proberen

Stel in hoe vaak een poging herhaald moet worden als die niet slaagt.

Duur voor opnieuw proberen

Als een gebeurtenis blijft herhalen en steeds niet slaagt, dan kunt u instellen hoe lang moet worden herhaald voordat de poging wordt opgegeven.

E-mailcontact

Voer een of meer e-mailadressen in waar e-mails met kennisgeving naartoe moeten worden verzonden als er een fout optreedt.

E-mailwaarschuwing verzenden na

Stel in hoe lang na het optreden van de fout de e-mail moet worden verzonden. Als het probleem is opgelost voordat deze tijd is verstreken en de gebeurtenis slaagt, dan wordt geen foutkennisgeving verzonden.

E-mailwaarschuwingen opnieuw verzenden

Stel in hoe vaak e-mails over fouten moeten worden verzonden als de fout blijft bestaan.

Uitgaande gebeurtenissen :: E-mail-geadresseerden

Nieuwe e-mailontvanger toevoegen, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

Huidige status

Geeft een kort statusbericht van de SMTP-relayserver weer. Zolang het apparaat berichten naar de relayserver kan verzenden, wordt de status als **OK** weergegeven. Anders moet u de instellingen van uw SMTP-relayserver controleren.

Duur voor opnieuw proberen

Als een gebeurtenis blijft herhalen en steeds niet slaagt, dan kunt u instellen hoe lang moet worden herhaald voordat de poging wordt opgegeven.

Uitgaande gebeurtenissen :: Geadresseerde voor e-mail toevoegen

Voordat u uw Bomgar Box instelt om berichten over gebeurtenissen naar een e-mailadres te verzenden, moet u controleren of uw Bomgar Box geconfigureerd om met uw SMTP-relayserver te werken. Ga naar de pagina **Beheer > E-mailconfiguratie** om de instellingen te controleren.

Naam

Maak een unieke naam aan om te helpen dit object te identificeren.

E-mailadres

Voer het e-mailadres in waarheen meldingen van geselecteerde gebeurtenissen moeten worden gezonden. U kunt maximaal tien e-mailadressen invoeren, gescheiden door komma's.

Uitgeschakeld

Gebruik het selectievakje **Uitgeschakeld** om snel berichten te stoppen voor de gebeurtenis-handler die u instelt, bijvoorbeeld wanneer u een geplande integratietest uitvoert.

Externe code vereisen

Als deze optie is aangevinkt, dan worden e-mails alleen verzonden voor sessies die een externe code hebben op het moment waarop de gebeurtenis optreedt.

Te verzenden gebeurtenissen

Kies welke gebeurtenissen berichten genereren die verzonden moeten worden.

Onderwerp

Pas het onderwerp van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Body

Pas de inhoud van deze e-mail aan. Gebruik de onder dit veld vermelde macro's op de pagina /login om de tekst aan uw wensen aan te passen.

Automatische omschakeling: Een back-up-apparaat instellen voor automatische omschakeling

Automatische omschakeling :: Configuratie

Nieuwe verbindingsdetails voor Backup-site: Hostnaam of IP-adres

Voer de hostnaam of het IP-adres in van de Bomgar Box die u als back-up wilt gebruiken in een relatie met automatische omschakeling.

TLS-Poort

Voer het TLS-poortnummer in waarmee dit primaire apparaat een verbinding met het back-up-apparaat kan maken.

Omgekeerde verbindingsdetails voor deze primaire site: Hostnaam of IP-adres

Voer de hostnaam of het IP-adres in van deze Bomgar Box die u als primair apparaat wilt gebruiken in een relatie met automatische omschakeling.

TLS-Poort

Voer het TLS-poortnummer in waarmee het back-up-apparaat een verbinding met dit primaire apparaat kan maken.

Automatische omschakeling :: Status

Status van deze host

Bekijk de hostnaam van deze site, samen met de status van de primaire site of van de back-up-site.

Status van peer-host

Bekijk de hostnaam van deze site, samen met de status van de primaire site of van de back-up-site. Bekijk ook de datum en het tijdstip van de laatste statuscontrole.

Statusgeschiedenis

Vouw een tabel met opgetreden statusgebeurtenissen uit of klap deze in.

Automatische omschakeling :: Status van de primaire of back-up-site

De tekst geeft een bevestiging dat u zich ofwel op de primaire site of op de back-up-site van uw hostsite bevindt.

Nu synchroniseren

Forceer handmatig een gegevenssynchronisatie vanaf het primaire apparaat naar het back-up-apparaat.

Back-up/primair worden

Verwissel met het andere apparaat van rol, waardoor in feite een automatische omschakeling wordt uitgevoerd voor gepland onderhoud of voor een bekende gebeurtenis die voor automatische omschakeling zorgt.

Vink dit vakje aan om een gegevenssynchronisatie uit te voeren vanaf de site op example.com terwijl deze back-up/primair wordt.

Als u de gegevens tussen de twee apparaten wilt synchroniseren voordat u de rollen verwisselt, dan moet u dit vakje aanvinken. Als deze optie wordt geselecteerd, dan wordt de verbinding met alle gebruikers op het primaire apparaat tijdens de gegevenssynchronisatie verbroken en zijn er geen nieuwe bewerkingen mogelijk totdat de rollen geheel verwisseld zijn.

Vink dit vakje aan om een back-up te worden, zelfs als geen verbinding kan worden gemaakt met het andere apparaat op example.com.

U hebt op de primaire site de optie om back-up te worden, zelfs als geen contact met het andere apparaat kan worden verkregen. Als deze optie niet is aangevinkt, dan wordt de automatische omschakeling geannuleerd als beide apparaten voor wat hun rollen bij automatische omschakeling betreft (één primair en één back-up) niet kunnen worden gesynchroniseerd.

Als u bijvoorbeeld weet dat het huidige back-up-apparaat online is maar vanwege verbindingsproblemen niet door het primaire apparaat kan worden bereikt, dan kunt u deze optie aanvinken om het primaire apparaat back-up te maken nog voordat de netwerkverbinding is hersteld. In dit voorbeeld hebt u ook toegang tot het back-up-apparaat nodig en moet u dat primair maken.

Relaties automatische omschakeling

Verbreek de relatie voor automatische omschakeling en verwijder elk van de apparaten van de rollen als primair c.q. back-up.

Automatische omschakeling :: Configuratie primaire of back-up-site

Gedeelde IP-adressen

Stel het gedeelde IP-adres in dat de site gebruikt in geval van een automatische omschakeling door het vakje voor het IP-adres voor automatische omschakeling aan te vinken. Als u de relatie tussen de sites wijzigt, dan worden de aangevinkte IP-adressen uitgeschakeld als een primaire site back-up wordt en ingeschakeld als een back-up-site primair wordt. U moet handmatig de instelling naar het andere apparaat kopiëren omdat de instelling niet wordt gedeeld.

Automatische omschakeling :: Instellingen voor back-up

De instellingen die u hier configureert worden alleen ingeschakeld als de site die u configureert als back-up functioneert.

Als u zich op de primaire site bevindt, selecteer dan **Instellingen voor back-up >** om de pagina met de te configureren velden uit of in te klappen.

Backupsitebewerkingen activeren

Schakel back-ups van de site in of uit.

Interval voor automatische data-synchronisatie

U kunt de tijden van het interval voor automatische gegevenssynchronisatie handmatig instellen.

Bandbreedtelimiet gegevenssynchronisatie

Stel de parameters in voor de bandbreedte tijdens gegevenssynchronisatie.

Automatische omschakeling activeren

Schakel de automatische omschakeling snel in of uit.

Time-out voor primaire site

Stel in hoe lang de primaire site onbereikbaar moet zijn voordat automatische omschakeling optreedt.

IP-adressen voor netwerkverbindingstest

Voer het IP-adres voor de back-up-site in om te bepalen of het back-up-apparaat het primaire apparaat niet kan bereiken omdat het primaire apparaat offline is of omdat het back-up-apparaat geen netwerkverbinding meer heeft.

API-configuratie: De XML API inschakelen en aangepaste velden configureren

API :: Configuratie

XML API activeren

U kunt ervoor kiezen de Bomgar XML API in te schakelen, waardoor u rapporten kunt maken en opdrachten kunt geven zoals het starten of verplaatsen van sessies vanuit externe toepassingen of om automatisch een back-up van uw softwareconfiguratie te maken.

***Opmerking**: Alleen de aanroepen **Opdracht**, **Rapportage** en **API voor clientscript** worden door deze instelling in- of uitgeschakeld. Andere API-aanroepen worden onder Publieke portalen geconfigureerd. Zie de API-programmeergids voor meer informatie.*

Toestemming voor HTTP-toegang tot XML API

Standaard is de toegang tot de API met SSL versleuteld. Maar u kunt ervoor kiezen niet-versleutelde HTTP-toegang toe te staan. Vanuit het oogpunt van beveiliging wordt sterk aanbevolen toegang via HTTP niet toe te staan.

API :: Aanpasbare velden

Maak aanpasbare API-velden aan om informatie over uw klant te verzamelen, waardoor u Bomgar beter kunt integreren met uw bestaande programma's. Aangepaste velden moeten in combinatie met de Bomgar API worden gebruikt. Zie de API-programmeergids voor meer informatie.

Nieuw veld aanmaken, bewerken, verwijderen

Maak een nieuw object aan, wijzig een bestaand object of verwijder een bestaand object.

API :: Aanpasbare velden :: Toevoegen of bewerken

Schermnaam

Maak een unieke naam aan om te helpen dit object te identificeren. De naam wordt in de toegangsconsole weergegeven als onderdeel van de sessiegegevens.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, wordt er automatisch een aangemaakt.

In toegangsconsole weergeven

Als u **In toegangsconsole weergeven** aanvinkt, dan zijn dit veld en de waarde ervan zichtbaar telkens wanneer de sessiegegevens in de toegangsconsole worden weergegeven.

Ondersteuning: Contact opnemen met Bomgar technische ondersteuning

Contactinformatie voor Bomgar ondersteuning

De ondersteuningspagina bevat contactinformatie voor het geval u contact wilt opnemen met een Bomgar technische klantendiensttechnicus.

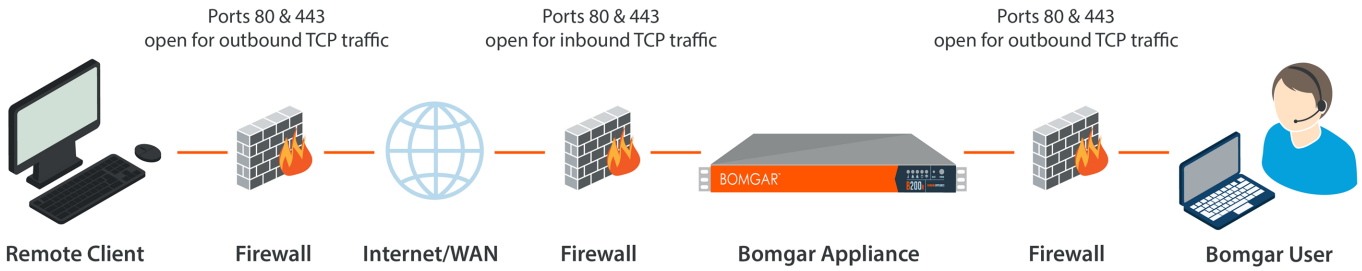
Geavanceerde technische ondersteuning van Bomgar

Mocht een Bomgar technische klantendiensttechnicus toegang tot uw apparaat nodig hebben, dan verstrekt hij of zij u codes voor ondersteuning, toegang en overschrijven die u op deze pagina kunt invoeren om een door het apparaat opgezet, volledig versleuteld ondersteuningskanaal terug naar Bomgar aan te maken om ingewikkelde problemen snel te kunnen oplossen.

Poorten en firewalls

Bomgar oplossingen zijn bedoeld om transparant door firewalls heen te werken en verbindingen met elke op internet aangesloten computer te maken, waar ook ter wereld. Maar bij bepaalde sterk beveiligde netwerken kan enige configuratie noodzakelijk zijn.

TYPICAL NETWORK SETUP: 15.1



- De poorten 80 en 443 moeten op de firewalls van het externe systeem en van de lokale gebruiken open staan voor uitgaand TCP-verkeer. Afhankelijk van het voor u samengestelde pakket moeten mogelijk meer poorten beschikbaar zijn. De afbeelding laat een normale netwerkinstelling zien. U kunt meer informatie hierover vinden in de Hardware-installatiegids voor Bomgar Boxen.
- Beveiligingssoftware voor internet zoals software firewalls mogen het downloaden van Bomgar uitvoerbare bestanden niet blokkeren. Voorbeelden van software firewalls zijn McAfee Security, Norton Security en Zone Alarm. Als u een software firewall hebt, dan krijgt u mogelijk verbindingsproblemen. Om zulke problemen te voorkomen, moet u de instellingen van uw firewall zodanig configureren dat de volgende uitvoerbare bestanden worden toegestaan. Hierin is {uid} een unieke identificator bestaande uit een letter en cijfers:
  - bomgar-pec-{uid}.exe
  - bomgar-pec.exe

  Neem contact op met de leverancier van uw firewall software voor assistentie.
- Voorbeelden van regels voor firewalls op basis van de locatie van een apparaat kunt u vinden op www.bomgar.com/docs/content/deployment/dmz/firewall-rules.htm.

Als u nog steeds problemen ondervindt bij het maken van een verbinding, neem dan contact op met Bomgar technische ondersteuning op help.bomgar.com.

Vrijwaringen, beperkingen voor licenties en technische ondersteuning

Vrijwaringen

Dit document is uitsluitend informatief. Bomgar behoudt zich het recht voor de inhoud ervan zonder voorafgaande kennisgeving te wijzigen. Bomgar geeft geen garantie dat dit document foutloos is en het bevat geen andere garanties of voorwaarden, al dan niet mondeling of wettelijk impliciet, inclusief impliciete garanties en voorwaarden voor verkoopbaarheid of geschiktheid voor een bepaald doel. Bomgar Corporation sluit expliciet elke aansprakelijkheid uit met betrekking tot dit document en het document vormt geen enkele contractuele verbintenis, direct noch indirect. De hierin beschreven technologieën, functionaliteit, services en processen kunnen zonder voorafgaande kennisgeving worden gewijzigd.

BOMGAR, BOMGAR BOX, mark B, JUMP en UNIFIED REMOTE SUPPORT zijn handelsmerken van Bomgar Corporation. Andere opgenomen handelsmerken zijn het eigendom van de respectievelijke eigenaren.

Licentiebeperkingen

Eén licentie voor Bomgar Privileged Access Management geldt voor toegang tot één eindpuntsysteem. Hoewel deze licentie van het ene systeem naar een ander systeem mag worden overgezet als toegang tot het eerste systeem niet langer nodig is, zijn twee of meer licenties (één per eindpunt) nodig om gelijktijdige toegang tot meerdere eindpunten mogelijk te maken.

Technische ondersteuning

We hebben bij Bomgar het commitment dat wij service van de allerhoogste kwaliteit bieden door ervoor te zorgen dat onze klanten alles hebben wat zij nodig hebben om zo productief mogelijk te kunnen werken. Als u assistentie nodig hebt, kunt u contact opnemen met Bomgar technische ondersteuning via help.bomgar.com.

Technische ondersteuning is beschikbaar wanneer de klant jaarlijks ons onderhoudsplan afneemt.