BOMGAR™

Privileged Access Management
Guida Amministrativa 15.3

TC:5/5/2016

Indice

Guida amministrativa di Privileged Access Management di Bomgar

Questa guida consente di avere una panoramica dettagliata di **/login** ed è progettata per l'amministrazione degli utenti Bomgar e del software Bomgar. Il dispositivo Bomgar funziona come punto centrale di amministrazione e gestione del software Bomgar e consente di connettersi da qualsiasi luogo provvisto di connessione Internet per scaricare la console di accesso.

Utilizzare questa guida solo dopo che l'amministratore ha completato l'impostazione e la configurazione iniziali del dispositivo Bomgar, come descritto dettagliatamente nella Guida all'installazione dell'hardware del dispositivo Bomgar. Una volta installato correttamente Bomgar, è possibile iniziare subito ad accedere agli endpoint. Per qualsiasi tipo di supporto, rivolgersi al supporto tecnico Bomgar all'indirizzo help.bomgar.com.

Login all'interfaccia amministrativa

Login

Connettersi all'interfaccia amministrativa utente dall'indirizzo URL del proprio dispositivo seguito da **/login**. L'interfaccia amministrativa utente consente agli amministratori di creare account utente e di configurare le impostazioni del software.

Anche se l'URL del dispositivo potrebbe essere qualsiasi DNS registrato, è molto probabile che sia un sottodominio del dominio principale dell'azienda (ad es., access.example.com/login).

Nome utente predefinito: **admin**

Password predefinita: **password**

Nota: *per motivi di sicurezza, il nome utente e la password amministrativi per l'interfaccia /appliance sono diversi da quelli per l'interfaccia /login e devono essere gestiti separatamente.*

Nota: *se l'autenticazione multifattore è stata abilitata per l'account, immettere il codice e-mail ricevuto. Se per tre volte consecutive viene immesso il codice e-mail errato, è necessario immettere di nuovo le credenziali e ottenere un nuovo codice e-mail.*

usa autenticazione browser integrata

Se Kerberos è stato correttamente configurato per l'accesso Single Sign-On, basta fare clic sul link di autenticazione integrata del browser per accedere direttamente all'interfaccia Web senza dover immettere le credenziali.

Hai dimenticato la tua password?

Se è stata abilitata la reimpostazione della password dalla **/login > Gestione > Sicurezza**, questo collegamento sarà visibile. Per reimpostare la password, fare clic sul collegamento, inserire il nome utente e rispondere correttamente alla domanda di sicurezza. Gli amministratori non possono reimpostare le proprie password utilizzando la domanda di sicurezza.

Accordo sui login

Gli amministratori possono limitare l'accesso alla schermata di login, consentendo che il Prerequisito Accordo sui login sia confermato prima che venga visualizzata la schermata di accesso. L'accordo di accesso può essere abilitato e personalizzato dalla pagina **/login > Gestione> Configurazione del sito**.

Stato

Informazioni: Visualizzazione dei dettagli del software Bomgar di Privileged Access Management

Stato del sito

La pagina principale dell'interfaccia Bomgar /login Privileged Access Management contiene una panoramica dei dati statistici relativi al dispositivo Bomgar. Quando si contatta il supporto tecnico Bomgar per gli aggiornamenti del software o per la risoluzione dei problemi, è possibile che venga richiesto di inviare un messaggio con la cattura di schermata di questa pagina.

Zona di fuso orario

Un amministratore è in grado di selezionare il fuso orario mediante l'apposito menu a discesa, impostando data e ora corrette del dispositivo per la regione selezionata.

Jump Client totali consentiti

Consente di visualizzare il numero totale di Jump Client attivi e passivi ammessi nel sistema. Questo numero viene stabilito dalla capacità hardware del dispositivo Bomgar.

Numero massimo di utenti simultanei

Consente di visualizzare il numero massimo di utenti che possono accedere contemporaneamente alla console di accesso. Questo numero viene stabilito dalla capacità hardware del dispositivo Bomgar.

Licenze dell'endpoint

Consente di visualizzare il numero di licenze disponibili nel dispositivo Bomgar. Gli endpoint includono Jump Client, collegamenti Jump remoti, collegamenti Jump locali, collegamenti RDP e Shell Jump. Se sono necessarie più licenze endpoint, rivolgersi alle Vendite Bomgar.

Endpoint configurati

Consente di visualizzare il numero di endpoint configurati nel dispositivo Bomgar. Gli endpoint includono Jump Client, collegamenti Jump remoti, collegamenti Jump locali, collegamenti RDP e Shell Jump.

Scarica Rapporto uso licenze

Consente di scaricare un file zip contenente informazioni dettagliate sull'utilizzo della licenza Bomgar. Il file contiene un elenco di elementi Jump (senza contare i Jump Client installati), il conteggio giornaliero delle operazioni dell'elemento Jump, l'utilizzo della licenza e un riepilogo dell'utilizzo e della varianza della licenza del dispositivo Bomgar e dell'endpoint.

Riavvia

È possibile riavviare il software Bomgar in modalità remota. Non riavviare il software se non per specifica richiesta del supporto tecnico Bomgar.

Il software del Client è costruito per provare

Questo è il nome host al quale si connette il software del client Bomgar. Se il nome host tentato dal software client deve essere cambiato, informare il supporto tecnico Bomgar dei cambiamenti necessari in modo che il supporto tecnico possa creare un aggiornamento software.

Client connessi

Visualizzare il numero e il tipo di client del software Bomgar connessi al dispositivo Bomgar.

Utenti: Visualizzazione degli utenti connessi e invio dei messaggi

Utenti connessi

Consente di visualizzare l'elenco degli utenti connessi alla console e l'ora in cui hanno eseguito il login e se stanno eseguendo sessioni.

Termina

È possibile interrompere la connessione dell'utente alla console di accesso.

Invia messaggio agli utenti

Nella console di accesso inviare un messaggio a tutti gli utenti connessi tramite una finestra popup.

Utenti Disponibilità estesa

Visualizzare gli utenti che hanno la modalità Disponibilità estesa abilitata.

Disabilita

È possibile disattivare la modalità Disponibilità estesa di un utente.

Mio account: Modificare password e nome utente, scaricare la console di accesso e altro software

Console di accesso Bomgar

Scegliere la piattaforma

Scegliere il sistema operativo sul quale installare il software. Questo menu a discesa passa automaticamente al programma di installazione previsto per il sistema operativo.

Scarica console di accesso Bomgar

Avvia Privileged Web, una console di accesso basata su Web.

Scaricare il programma di installazione della console di accesso Bomgar.

Per gli amministratori di sistema che devono fornire il programma di installazione della console a molti sistemi, il programma di installazione Microsoft può essere utilizzato con il proprio strumento di gestione dei sistemi. Nel prompt dei comandi, quando si digita il comando per installare la console utilizzando l'opzione MSI, passare alla directory dove è stato scaricato l'MSI e immettere il comando incluso nella pagina **Mio account**.

Per l'installazione MSI è possibile impostare parametri opzionali.

- **INSTALLDIR=** accetta qualsiasi percorso valido della directory dove si desidera installare la console.
- **RUNATSTARTUP=** accetta **0** (impostazione predefinita) o **1**. Con l'impostazione 1, la console viene eseguita ogni volta che si avvia il computer.
- **ALLUSERS=** accetta **""** o **1** (impostazione predefinita). Con l'impostazione **1**, la console viene installata per tutti gli utenti del computer; altrimenti viene installata solo per l'utente corrente.
- **SHOULDAUTOUPDATE=1** Se la si installa solo per l'utente corrente, si può scegliere l'aggiornamento automatico della console in caso di aggiornamento del sito, immettendo il parametro 1; il valore **0** (impostazione predefinita) non consente l'aggiornamento automatico ed esige la reinstallazione manuale della console in caso di aggiornamento del sito. Se viene installata per tutti gli utenti, la console non si aggiorna automaticamente.

Smart card virtuale Bomgar

Per tentare l'autenticazione della smart card virtuale, l'utente Bomgar deve avere il driver della smart card virtuale Bomgar installato. Il computer al quale si accede deve funzionare in modalità elevata. Inoltre, deve avere il driver della smart card virtuale dell'endpoint Bomgar installato oppure deve essere accessibile dalla funzionalità Esegui il Jump su della console di accesso. Per maggiori dettagli e requisiti, consultare il documento Smart card per l'autenticazione remota.

Scegliere architettura Windows

Selezionare questa opzione per scaricare il programma di installazione della smart card virtuale per il sistema dell'utente Bomgar o dell'endpoint.

Scarica programma di installazione della smart card virtuale

Scaricare il programma di installazione della smart card virtuale selezionato in precedenza. Una smart card virtuale consente di autenticarsi su un sistema remoto utilizzando una smart card sul sistema locale.

Servizio di elevazione automatica Bomgar

Scegliere architettura Windows

Scegliere il sistema operativo sul quale installare il software. Questo menu a discesa passa automaticamente al programma di installazione previsto per il sistema operativo.

Scarica programma di installazione del servizio di elevazione automatica

In casi particolari, può essere necessario avviare una sessione con il client dell'endpoint già in modalità elevata oppure elevare il client dell'endpoint senza fornire le credenziali. Per elevare in modo sicuro il client dell'endpoint, senza il prompt, scaricare il **Servizio di elevazione automatica Bomgar** e installarlo prima sui sistemi Windows remoti per i quali è necessario l'accesso di elevazione senza credenziali. È necessario installare il servizio elevazione utilizzando un account con privilegi amministrativi sulla macchina locale.

Quando il servizio di elevazione viene eseguito, si aggiunge al registro un hash univoco del sito Bomgar. Poi, quando il sistema utente remoto avvia una sessione da quel sito, il servizio elevazione verifica la corrispondenza dell'hash del registro con l'hash del client. Se corrispondono, il client tenta l'elevazione automatica.

Scarica file di registro del servizio di elevazione automatica

Dopo un aggiornamento del software Bomgar, la hash del sito cambia. Scaricare ed eseguire il file di registro del servizio elevazione per aggiornare la hash Registro su sistemi che hanno già il servizio elevazione installato. È necessario eseguire il servizio elevazione utilizzando un account con privilegi amministrativi sulla macchina locale.

Modalità Disponibilità estesa

Abilita o Disabilita

Abilitare o disabilitare la modalità Disponibilità estesa facendo clic sul pulsante **Abilita/Disabilita**. La modalità Disponibilità estesa consente di ricevere e-mail di invito da altri utenti che chiedono di condividere una sessione quando non si è connessi alla console di accesso.

Modifica le impostazioni e-mail

Indirizzo e-mail

Impostare un indirizzo e-mail per ricevere le e-mail di notifica, quali reimpostazione password o gli avvisi di modalità Disponibilità estesa.

Lingua preferita per e-mail

Se in questo sito è abilitata più di una lingua, impostare la lingua da utilizzare per l'invio di e-mail.

Cambia la tua password

Bomgar consiglia di cambiare regolarmente la password.

Nome utente, Password attuale, Nuova password

Verificare di essere entrati nell'account del quale si desidera modificare la password e poi immettere la password corrente. Creare e confermare una nuova password per l'account. La password può essere impostata su qualsiasi valore premesso che la stringa rientri nei limiti definiti nella procedura impostata nella pagina **/login > Gestione > Sicurezza**.

Cambia la tua domanda/risposta di sicurezza

Domanda e risposta di sicurezza

La domanda e la risposta di sicurezza consentono di resettare una password dimenticata dopo aver fornito la risposta esatta a questa domanda. Le password devono essere reimpostate solo se è selezionata l'opzione **Abilita reimpostazione password** nella pagina **Gestione > Sicurezza**. Gli amministratori non possono reimpostare le proprie password utilizzando la domanda di sicurezza.

Configurazione

Opzioni: Gestire opzioni di connessione, Registra sessioni

Opzioni di sessione

Richiedi sessioni chiuse in logout o esci

Se si seleziona **Richiedi sessioni chiuse al logout o Esci**, gli utenti non sono in grado di disconnettersi dalla console fino a quando le schede della sessione sono aperte.

Opzioni di connessione

Time-out per riconnessione

Determinare per quanto tempo un client endpoint disconnesso deve tentare di riconnettersi.

Limitare l'accesso fisico all'endpoint se l'endpoint perde la connessione o se tutti gli utenti della sessione sono scollegati

Se la connessione della sessione cade, l'input di mouse e tastiera del sistema remoto può essere temporaneamente disattivato, per essere ripristinato quando la connessione viene ristabilita o la sessione terminata.

Comportamento di Termina sessione

Se risulta impossibile ristabilire la connessione entro il tempo impostato dal **Time-out per riconnessione**, selezionare l'azione da eseguire. Per impedire a un utente finale di acquisire privilegi non autorizzati dopo una sessione elevata, impostare il client in modo da disconnettere automaticamente l'utente finale dal computer Windows remoto a fine sessione oppure bloccare il computer remoto o non fare nulla. Queste regole non si applicano a sessioni di condivisione del browser.

Consenti agli utenti di annullare questa impostazione per-sessione

È possibile consentire a un utente di annullare l'impostazione di termine sessione mediante la scheda **Riepilogo** nella console durante una sessione.

Opzioni di logging della sessione di accesso

Abilita condivisione schermo / Registrazione shell di comando

Scegliere se si desidera registrare automaticamente come video le sessioni di condivisione schermo e/o le sessioni della shell di comando. L'attivazione di registrazioni della shell di comando consente inoltre che le sessioni della shell di comando siano

disponibili come trascrizioni di testo.

Condivisione schermo / Risoluzione registrazione shell di comando

Impostare la risoluzione di riproduzione della registrazione della sessione.

> ***Nota:*** *tutte le registrazioni vengono salvate in formato raw; i valori della risoluzione riguardano solo la riproduzione.*

Abilita il Logging automatico delle informazioni del sistema

Scegliere se recuperare automaticamente le informazioni di sistema dal sistema remoto all'inizio della sessione in modo che siano disponibili successivamente nei dati del report di sessione.

Abilita Sessione Forensic

Scegliere se si desidera la capacità aggiunta per la ricerca in tutte le sessioni in base agli eventi di sessione, che includono messaggi di chat, il trasferimento di file, gli eventi dell'editor del registro e gli eventi modificati della finestra in primo piano della sessione. Questa funzione è abilitata per impostazione predefinita.

> ***Nota:*** *se la shell di comando è attivata, Sessione Forensic consente all'utente di fare una ricerca approfondita delle registrazioni shell. Quando si cerca un termine chiave viene fatta una corrispondenza in una registrazione della shell memorizzata, il video viene automaticamente messo in coda in quel punto della registrazione. Non vengono registrati output di comando o password.*

Team: Raggruppare gli utenti in team

Team :: Gestisci

Raggruppare gli utenti in team consente di assegnare in modo efficiente la gestione tra i gruppi di utenti. Nella console di accesso ogni team viene visualizzato come coda separata per le sessioni.

Aggiungi nuovo team, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente. L'eliminazione di un team non cancella gli account degli utenti, ma solo la loro associazione al team.

Team :: Aggiungi o Modifica

Impostazioni generali

Nome del team

Creare un nome univoco per consentire di identificare questo oggetto.

Nome codice

Impostare un nome codice a scopi di integrazione. Se non si imposta un nome codice, ne verrà creato uno automaticamente.

Commenti

Inserire commenti per aiutare a identificare la finalità dell'oggetto.

Procedure di gruppo

Annotarsi le procedure di gruppo che assegnano membri a questo team. Fare clic sul collegamento alla pagina **Procedure di gruppo** per verificare o assegnare membri delle procedure.

Membri del team

Selezionare uno o più utenti nell'elenco degli utenti disponibili e fare clic sulla freccia per spostarli nel team.

Il ruolo degli agenti di un team può essere impostato come **membro**, **coordinatore** o **manager**. Questi ruoli svolgono una funzione importante nel **Dashboard** della console di accesso.

I membri del team che condividono l'appartenenza tramite una o più procedure di gruppo vengono elencati insieme a un collegamento alla pagina di configurazione **Procedure di gruppo**.

Accesso al Jump Client

Accesso autorizzato da questo team

Selezionare i team che devono accedere ai Jump Client vincolati al gruppo Jump del team. Per impostazione predefinita, solo questo team può accedere ai propri Jump Client. È comunque possibile selezionare altri team per visualizzare ed eseguire il Jump ai Jump Client di questo team.

Accesso autorizzato a questo team

Visualizzare un elenco di altri team che condividono l'accesso al Jump Client con i membri di questo team.

Team :: Impostazioni Dashboard

All'interno di un team, un utente può amministrare solo gli altri con ruoli inferiori al suo. Tenere presente, tuttavia, che i ruoli valgono esclusivamente nell'ambito di un team, pertanto un utente può essere in grado di amministrare un altro utente del suo team, ma non lo stesso utente in un altro team.

Monitoraggio dei membri del team nel dashboard

Se l'opzione è attivata, il coordinatore o il gestore di un team possono monitorare il team dal dashboard. Scegliere una selezione per **Disattivare** la possibilità di monitorare oppure scegliere **Solo console di accesso** per consentire al coordinatore o manager di un team di monitorare la console di accesso di un membro del team. Il monitoraggio coinvolge i Coordinatori e i Gestori di tutti i team sul sito.

Abilita Trasferimento sessione e Subentra alla guida in Dashboard

Se questa opzione è selezionata, un Coordinatore del team può anche subentrare alla guida di o trasferire una sessione di un membro del team. Analogamente, il manager di un team può amministrare coordinatori e membri del team.

Jump

Jump Clients: Gestione delle impostazioni e installazione di Jump Client per l'accesso all'endpoint

Guida all'utilizzo di massa del Jump Client

La procedura guidata di distribuzione di massa consente agli amministratori e agli utenti muniti dei necessari privilegi di distribuire Jump Client in uno o più computer remoti per l'accesso non assistito in un momento successivo.

Consenti l'override durante l'installazione

Alcune impostazioni della Procedura guidata alla distribuzione di massa consentono la sovrascrittura, abilitando l'utilizzo della riga di comando per impostare i parametri specifici della distribuzione prima dell'installazione.

Gruppo Jump

Dal menu a discesa selezionare se vincolare il Jump Client al gruppo Jump personale o al gruppo Jump generale. Vincolare il client al proprio gruppo Jump personale significa acquisire l'esclusività dell'accesso a questo computer remoto tramite il proprio Jump Client. Se si esegue il vincolo a un gruppo Jump del team, questo Jump Client diventa disponibile a tutti i membri del team che hanno accesso ai Jump Client del team.

Procedura Jump

È possibile applicare una **procedura di sessione** a questo Jump Client. Le procedure di sessione vengono configurate nella pagina **Jump >Procedure Jump** e stabiliscono gli orari durante i quali un utente può accedere al Jump Client. Una procedura Jump può inviare anche una notifica quando vi si accede o può richiedere l'approvazione per l'accesso. Se non si applica alcuna procedura Jump, è possibile accedere a questo Jump Client senza limitazioni.

Tag

L'aggiunta di un **tag** agevola l'organizzazione di Jump Client in categorie nella console di accesso.

Tipo di Connessione

Imposta **Tipo di connessione** su **Attivo** o **Passivo** per consentire l'installazione di Jump Client.

Proxy del Jumpoint

Se uno o più Jumpoint è impostato come proxy, è possibile selezionare un Jumpoint che funga da proxy per queste connessioni Jump Client. In tal modo, se sono installati in computer privi di connessione Internet nativa, questi Jump Client possono utilizzare il Jumpoint per riconnettersi al dispositivo Bomgar. I Jump Client devono essere installati sulla stessa rete del Jumpoint selezionato come proxy per le connessioni.

Commenti

Aggiungere **Commenti**, per semplificare la ricerca e l'identificazione di computer remoti. Tenere presente che tutti i Jump Client distribuiti mediante questo programma di installazione avranno gli stessi commenti impostati inizialmente, se non è selezionata l'opzione **Consenti sovrascrittura durante l'installazione** e si utilizzano i parametri disponibili per modificare il programma di installazione per le singole installazioni.

Il programma di installazione è valido per

Il programma di installazione resta utilizzabile solo per il tempo specificato dal menu a discesa **Questo programma di installazione è valido per**. Accertarsi di lasciare tempo sufficiente per l'installazione. Se si tenta di eseguire il programma di installazione di Jump Client dopo la scadenza del termine, l'installazione non riesce ed è necessario creare un nuovo programma di installazione. Il periodo può essere impostato su valori che vanno da 10 minuti a 1 anno. Questa impostazione NON ha niente a che vedere con il periodo in cui il Jump Client rimane attivo.

Tenta di effettuare un'installazione di grado superiore se il client la supporta

Se si seleziona **Tenta installazione elevata se il client la supporta**, il programma di installazione viene eseguito con diritti amministrativi e il Jump Client viene installato come un servizio di sistema. Se il tentativo di installazione elevata non riesce o se questa opzione è deselezionata, il programma di installazione viene eseguito con diritti amministrativi e il Jump Client viene installato come una qualsiasi applicazione. Questa opzione si applica solo a sistemi operativi Windows e Mac.

> ***Nota:*** *un Jump Client vincolato in modalità utente è disponibile solo quando è connesso tale utente. Al contrario, un Jump Client vincolato in modalità servizio con diritti elevati consente che il sistema sia sempre disponibile a prescindere dall'utente connesso.*

Richiedi l'elevazione delle credenziali se necessario

Se viene selezionata l'opzione **Chiedi elevazione credenziali se necessario**, il programma di installazione invita l'utente a inserire le credenziali amministrative, se il sistema esige che tali credenziali siano fornite in modo indipendente; in caso contrario, procederà all'installazione di Jump Client con diritti utente. Ciò si applica soltanto se si tenta un'installazione elevata.

Avvia il client dell'endpoint ridotto a icona quando si avvia la sessione

Selezionando **Avvia client dell'endpoint ridotto a icona quando si avvia la sessione**, il client dell'endpoint non viene visualizzato in primo piano e resta ridotto a icona nella barra delle applicazioni o ancorato quando una sessione viene avviata mediante uno di questi Jump Client.

Guida alla distribuzione

Per gli amministratori di sistema che devono fornire il programma di installazione di Jump Client a molti sistemi, l'eseguibile di Windows, Mac, Linux o Windows MSI può essere utilizzato con un qualsiasi strumento di gestione dei sistemi. È possibile includere un percorso valido per la directory personalizzata dove si desidera installare il Jump Client. È anche possibile sovrascrivere determinati parametri di installazione specifici a seconda delle proprie esigenze. Questi parametri si possono specificare per MSI ed EXE utilizzando lo strumento di amministrazione dei sistemi o l'interfaccia della riga di comando. Quando si contrassegnano le opzioni di installazione specifiche per la sovrascrittura durante l'installazione, è possibile utilizzare i seguenti parametri facoltativi per modificare il programma di installazione di Jump Client per installazioni individuali. Tenere presente che se un parametro viene passato nella riga di comando, ma non viene contrassegnato per la sovrascrittura nell'interfaccia amministrativa /login, l'installazione non riesce. Se l'installazione non riesce, visualizzare il registro del sistema operativo per verificare eventuali errori di installazione.

Parametro della riga di comando	Valore	Descrizione
--install-dir	<directory_path>	Specifica una nuova directory scrivibile dove installare il Jump Client. È supportata soltanto su Windows e Linux. Quando si definisce una directory di installazione personalizzata, accertarsi che la directory che si sta creando non esista già e che si trovi in una posizione che si possa scrivere.
--jc-jump-group	user:<username> team:<team-code-name>	Se la sovrascrittura è consentita, questo parametro della riga di comando sovrascrive il gruppo Jump indicato nella Procedura guidata alla distribuzione di massa.
--jc-session-policy	<session-policy-code-name>	Se la sovrascrittura è consentita, questo parametro della riga di comando imposta la procedura di sessione del Jump Client che controlla la procedura di autorizzazione durante una sessione di accesso.
--jc-jump-policy	<jump-policy-code-name>	Se la sovrascrittura è consentita, questo parametro della riga di comando imposta la procedura Jump che controlla le modalità di Jump degli utenti al Jump Client.
--jc-tag	<nome tag>	Se la sovrascrittura è consentita, questo parametro della riga di comando imposta il tag del Jump Client.
--jc-comments	<comments ... >	Se la sovrascrittura è consentita, questo parametro della riga di comando imposta i commenti del Jump Client.

Nota: *quando si distribuisce un programma di installazione MSI su Windows utilizzando il comando msiexec, i parametri precedenti si possono specificare mediante:*

1. *Rimozione dei trattini iniziali (-)*
2. *Conversione dei trattini rimanenti in caratteri di sottolineatura (_)*
3. *Assegnazione di un valore utilizzando un segno di uguale (=)*

Esempio:

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

La sola eccezione a questa regola è ***installdir****, che ha un trattino nella versione EXE, ma nessun trattino nella versione MSI.*

Scarica o installa il client ora

Piattaforma

Scegliere il sistema operativo sul quale installare il software. Questo menu a discesa passa automaticamente al programma di installazione previsto per il sistema operativo.

Tenere presente che, a differenza della console di accesso, i Jump Client installati con un MSI eseguono l'aggiornamento automatico.

Scarica/Installa

È possibile scaricare e installare immediatamente il Jump Client se si è al computer che sarà utilizzato successivamente per l'accesso.

Invia a destinatari email

Email

Si può anche inviare per e-mail il programma di installazione a uno o più utenti remoti. Più destinatari possono installare il client mediante lo stesso link.

Dati Jump Client

Un amministratore può scegliere quali dati visualizzare per tutti i Jump Client su un intero sito. Queste statistiche vengono visualizzate nella console di accesso e comprendono sistema operativo, tempi d'utilizzo, utente console, CPU, utilizzo del disco e un'anteprima della schermata remota. I Jump Client esistenti non influiscono sulle modifiche alle statistiche del Jump Client nel successivo intervallo di aggiornamento.

Impostazioni Jump Client

Intervallo di aggiornamento attivo statistiche Jump

L'**Intervallo di aggiornamento attivo statistiche Jump Client** determina la frequenza di aggiornamento di tali dati. La gestione del tipo di dati da visualizzare e della frequenza di visualizzazione può agevolare la regolamentazione della quantità di ampiezza di banda utilizzata. Più numerosi sono i Jump Client attivi installati, minori sono i dati e più ampio è l'intervallo che potrebbe essere necessario.

Numero massimo di aggiornamenti simultanei di Jump Client

Impostare anche il numero massimo di Jump Client che possono eseguire l'aggiornamento contemporaneamente. Va notato che se i Jump Client installati sono numerosi, potrebbe essere necessario limitarne il numero per regolamentare la quantità di ampiezza di banda consumata.

> ***Nota:*** *l'impostazione non condiziona gli upgrade della console di accesso.*

Larghezza di banda massima degli aggiornamenti simultanei di Jump Client

Si può anche regolare la larghezza di banda utilizzata durante gli aggiornamenti impostando l'opzione **Larghezza di banda massima di aggiornamenti simultanei di Jump Client**.

> ***Nota:*** *l'impostazione non condiziona gli upgrade della console di accesso.*

Consenti l'accesso simultaneo di più utenti a un solo Jump Client

L'opzione **Consenti l'accesso simultaneo di utenti a un singolo Jump Client** offre a più utenti la possibilità di ottenere l'accesso simultaneo allo stesso Jump Client senza dover essere invitati da un altro utente a partecipare a una sessione attiva. Il primo utente che accede al Jump Client mantiene la titolarità della sessione. Gli utenti che partecipano a una sessione Jump condivisa possono vedersi e conversare.

Nota: *questa impostazione (implementata solo in Windows) impedisce a un cliente di disattivare o disinstallare un Jump Client dal computer locale utilizzando il menu contestuale con il tasto destro del mouse sul tray del sistema. Per eliminare il Jump Client, gli utenti con i privilegi idonei sul computer del client possono farlo utilizzando la funzionalità standard di Windows Aggiungi/Rimuovi programmi. Se questa impostazione viene modificata, viene riapplicata a un Jump Client la volta successiva che si connette al dispositivo.*

Consente all'utente di tentare di riattivare i Jump Client

L'opzione **Consenti agli utenti il wake-up dei Jump Client** consente di eseguire il wake-up di un Jump Client selezionato trasmettendo i pacchetti Wake-on-LAN (WOL) su un altro Jump Client sulla stessa rete. Dopo aver tentato un WOL, l'opzione non sarà disponibile per 30 secondi prima di effettuare il tentativo successivo. I pacchetti WOL devono essere abilitati sul computer di destinazione e sulla rete per consentire che la funzione sia attiva. Le informazioni sul gateway predefinito del Jump Client vengono utilizzate per stabilire se altri Jump Client sono presenti nella stessa rete. Quando si invia un pacchetto WOL, l'utente dispone di un'opzione avanzata per fornire una password per gli ambienti WOL che richiedono una password WOL sicura.

Tipo di connessione predefinita di Jump Client

Impostare se il tipo di connessione del Jump Client predefinito deve essere attivo o passivo.

Porta del Jump Client passivo

La **Porta Jump Client passivo** indica la porta utilizzata dal Jump Client passivo per ascoltare un comando "wake up" del dispositivo. La porta predefinita è 5832. Accertarsi che le impostazioni del firewall consentano il traffico in entrata su questa porta per gli host con Jump Client passivi. Dopo l'attivazione, i Jump Client si connettono sempre al dispositivo sulla porta in uscita 80 oppure 443.

Procedure Jump: Impostare pianificazioni, notifiche e approvazioni per gli elementi Jump

Procedure Jump

Aggiungi nuova procedura Jump, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Procedure Jump :: Aggiungi

Nome display

Creare un nome univoco per consentire di identificare questo oggetto. Questo nome aiuta gli utenti a identificare la procedura durante l'assegnazione ai Jump Client.

Nome codice

Impostare un nome codice a scopi di integrazione. Se non si imposta un nome codice, ne verrà creato uno automaticamente.

Descrizione

Aggiungere una breve descrizione per riassumere lo scopo di questo oggetto.

Programma Jump: Abilitato

Impostare una pianificazione per stabilire quando è possibile accedere ai Jump Client con questa procedura. Impostare il fuso orario da utilizzare per la programmazione e aggiungere una o più voci di programmazione. Per ciascuna voce, immettere il giorno e l'ora di inizio e il giorno e l'ora di fine.

Se, ad esempio, è stato impostato l'inizio alle ore 8.00 e la fine alle ore 17.00, un utente può avviare una sessione utilizzando questo Jump Client in qualsiasi momento durante questa finestra temporale, ma può continuare a lavorare oltre il limite di fine impostato. Tuttavia non potrà riaccedere al Jump Client dopo le 17.00.

Forza il termine della sessione quando la pianificazione non consente l'accesso

Se è richiesto il controllo più rigoroso degli accessi, selezionare l'opzione **Forza il termine della sessione**. In tal modo la sessione viene disconnessa all'ora di fine pianificata. In questo caso, l'utente inizia a ricevere notifiche ripetute 15 minuti prima della disconnessione.

Notifica Jump: Avverte i destinatari quando viene avviata una sessione

Se questa opzione è selezionata, viene inviata un'e-mail di notifica ai destinatari designati se viene avviata una sessione con un Jump Client che utilizza questa procedura Jump. Quando un utente tenta di avviare una sessione con un Jump Client che utilizza

questa procedura, un prompt dichiara che sarà inviata una notifica via e-mail e chiede se l'utente desidera avviare comunque la sessione.

Avverte i destinatari quando viene terminata una sessione

Se questa opzione è selezionata, viene inviata un'e-mail di notifica ai destinatari designati se viene terminata una sessione con un Jump Client che utilizza questa procedura Jump. Quando un utente tenta di avviare una sessione con un Jump Client che utilizza questa procedura, un prompt dichiara che alla fine della sessione sarà inviata una notifica via e-mail e chiede se l'utente desidera avviare comunque la sessione.

Indirizzi e-mail

Inserire uno o più indirizzi e-mail ai quali essere inviati le e-mail. Separare gli indirizzi con uno spazio. Questa funzione richiede una valida configurazione SMTP per il dispositivo, da impostare nella pagina **/login > Gestione > Configurazione e-mail**.

Nome display

Inserire il nome del destinatario dell'e-mail. Questo nome viene visualizzato nel prompt che l'utente riceve prima di una sessione con un Jump Client che utilizza questa procedura.

Impostazioni internazionali

Se in questo sito è abilitata più di una lingua, impostare la lingua da utilizzare per l'invio di e-mail.

Approvazione Jump: Richiede un ID ticket prima dell'inizio di una sessione

Se questa opzione è selezionata, l'utente deve inserire un ID ticket valido prima di iniziare una sessione di accesso. Quando tenta di accedere a un endpoint con questa procedura Jump applicata, l'utente deve inserire un ID ticket dall'ITSM esistente oppure dal processo di approvazione dell'ID ticket prima che venga concesso l'accesso. Configurare l'ITSM o l'integrazione del sistema ticket dalla sezione **Procedure Jump :: Sistema ticket**.

Richiede l'approvazione prima dell'inizio di una sessione

Se questa opzione è selezionata, viene inviata un'e-mail di approvazione ai destinatari designati se si tenta una sessione con un Jump Client che utilizza questa procedura Jump. Quando un utente tenta di avviare una sessione con un elemento Jump che utilizza questa procedura, una finestra di dialogo chiede all'utente di inserire il motivo della richiesta, l'ora e la durata della richiesta.

Durata massima di accesso

Impostare il tempo massimo consentito a un utente per richiedere accesso a un Jump Client che utilizza questa procedura. L'utente può richiedere un tempo inferiore di accesso non superiore a quello impostato in questa sede.

Indirizzi e-mail

Inserire uno o più indirizzi e-mail ai quali essere inviati le e-mail. Separare gli indirizzi con uno spazio. Questa funzione richiede una valida configurazione SMTP per il dispositivo, da impostare nella pagina **/login > Gestione > Configurazione e-mail**.

Nome display

Inserire il nome del destinatario dell'e-mail. Questo nome viene visualizzato nel prompt che l'utente riceve prima di una sessione con un Jump Client che utilizza questa procedura.

Impostazioni internazionali

Se in questo sito è abilitata più di una lingua, impostare la lingua da utilizzare per l'invio di e-mail.

Procedure Jump :: Modello notifica e-mail

Oggetto

Personalizzare l'oggetto di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Testo

Personalizzare il corpo di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Procedure Jump :: Modello approvazione e-mail

Oggetto

Personalizzare l'oggetto di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Testo

Personalizzare il corpo di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Procedure Jump :: Sistema ticket

URL del sistema ticket

Nell'**URL sistema ticket**, inserire l'URL del sistema ticket esterno. Il dispositivo Bomgar invia una richiesta in uscita al sistema ticket esterno. L'URL deve essere formattato per HTTP e HTTPS. Se viene inserito un URL HTTPS, il certificato del sito deve essere verificato per una connessione valida. Se esiste una procedura Jump che richiede un ID ticket, l'URL del sistema ticket deve essere inserito oppure si riceve un messaggio di avvertenza.

Stato attuale

Il campo **Stato attuale** viene visualizzato solo quando esiste un valore di stato valido per segnalare la connessione al sistema ticket configurato nell'**URL del sistema ticket**. La modifica della configurazione del sistema ticket reimpostata il valore.

Carica un certificato per le connessioni HTTPS

Fare clic su **Seleziona file** per caricare il certificato per la connessione del sistema ticket HTTPS al dispositivo. Se il certificato è caricato, il dispositivo lo utilizza quando contatta il sistema esterno. Se il certificato non viene caricato ed è selezionata la casella

sotto l'impostazione **Ignora errori certificato SSL**, il dispositivo Bomgar torna a utilizzare l'archivio di certificati incorporati quando invia la richiesta.

Ignora errori del certificato SSL

Se l'opzione è selezionata, il dispositivo Bomgar **non** include le informazioni di convalida del certificato quando contatta il sistema ticket esterno. Lasciare questa casella non selezionata se si sta caricando un certificato per le connessioni HTTPS protette.

Prompt utente

In **Prompt utente** inserire il testo della finestra di dialogo che gli utenti della console di accesso devono visualizzare quando viene chiesto di inserire l'ID ticket necessario per l'accesso.

Jumpoint: Impostare un accesso non assistito a una rete

Gestione Jumpoint

La tecnologia Jump di Bomgar consente a un utente di accedere a computer su una rete remota senza dover preinstallare il software in ogni macchina. Basta installare un singolo tecnico di supporto Jumpoint in qualsiasi punto di una rete per ottenere l'accesso non assistito a ogni PC nell'ambito della rete.

Aggiungi nuovo Jumpoint, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Ridistribuisci

Disinstallare un Jumpoint esistente e scaricare un programma di installazione per sostituire il Jumpoint esistente con uno nuovo. I collegamenti Jump associati a un Jumpoint esistente utilizzano il nuovo Jumpoint una volta installato.

Nota: *quando un Jumpoint viene sostituito, la configurazione non viene salvata. Il nuovo Jumpoint deve essere riconfigurato.*

Jumpoint :: Aggiungi o Modifica

Nome

Creare un nome univoco per consentire di identificare questo oggetto. Questo nome consente agli utenti di individuare questo Jumpoint quando devono iniziare una sessione con un computer nella stessa rete.

Nome codice

Impostare un nome codice a scopi di integrazione. Se non si imposta un nome codice, ne verrà creato uno automaticamente.

Disabilitato

Se questa opzione è selezionata, il Jumpoint non è disponibile per eseguire connessioni Jump.

Gruppo

Se questa opzione è selezionata, l'utente è in grado di aggiungere più nodi ridondanti dello stesso Jumpoint su diversi sistemi host. Ciò assicura che fino a quando resta online almeno un nodo, il Jumpoint è disponibile.

Abilita metodo Shell Jump

Se si desidera che gli utenti si connettano a dispositivi di rete attivati per SSH e Telnet mediante questo Jumpoint, selezionare **Abilita accesso Shell Jump**.

Aggiungi utenti

Dalla pagina di modifica del Jumpoint, è possibile autorizzare gli utenti per avviare le sessioni mediante questo Jumpoint. Dopo la creazione del Jumpoint, è possibile anche concedere l'accesso a gruppi di utenti nella scheda **Utenti e sicurezza > Procedure di gruppo**.

Procedura guidata per l'importazione di massa di collegamenti Jump

Quando si creano molti collegamenti Jump, può risultare più semplice importarli mediante un foglio di calcolo piuttosto che aggiungerli uno a uno alla console di accesso. Dal menu a discesa **sezione procedura guidata Importazione di massa dei collegamenti Jump**, selezionare il tipo di elemento Jump da aggiungere e fare clic su **Scarica modello**. Utilizzare il testo del modello CSV come intestazione di colonna per aggiungere le informazioni per ogni collegamento Jump da importare. Si possono compilare o lasciare vuoti altri campi facoltativi.

Dopo aver completato il modello, utilizzare **Importa collegamenti Jump** per caricare il file CSV contenente le informazioni sull'elemento Jump. È possibile includere un solo tipo di elemento Jump in ogni file CSV. Il file CSV deve essere nel formato descritto nelle tabelle seguenti. La dimensione massima del file da caricare in una sola volta è 5 MB.

Collegamento Jump locale

Campo	Descrizione
Nome Host	Nome host dell'endpoint a cui si accede con questo collegamento Jump.
Gruppo Jump	Nome codice del team a cui si deve associare questo elemento Jump. ***Nota:*** *se si utilizza il metodo di importazione, non è possibile associare un elemento Jump a un gruppo Jump personale.*
Tag (opzionale)	È possibile organizzare gli elementi Jump in categorie aggiungendo un tag. Questa stringa ha un massimo di 1024 caratteri.
Commenti (opzionali)	È possibile aggiungere commenti ai propri elementi Jump. Questa stringa ha un massimo di 1024 caratteri.
Procedura Jump (opzionale)	Nome codice di una procedura Jump. È possibile specificare una procedura Jump per gestire l'accesso a questo elemento Jump.
Procedura di sessione (opzionale)	Nome codice di una procedura di sessione. È possibile specificare una procedura di sessione per gestire le autorizzazioni disponibili su questo elemento Jump.

Collegamento Jump remoto

Campo	Descrizione
Nome Host	Nome host dell'endpoint a cui si accede con questo collegamento Jump.

Campo	Descrizione
Jumpoint	Nome codice del Jumpoint che l'endpoint utilizza per l'accesso.
Gruppo Jump	Nome codice del team a cui si deve associare questo elemento Jump. ***Nota:*** *se si utilizza il metodo di importazione, non è possibile associare un elemento Jump a un gruppo Jump personale.*
Tag (opzionale)	È possibile organizzare gli elementi Jump in categorie aggiungendo un tag. Questa stringa ha un massimo di 1024 caratteri.
Commenti (opzionali)	È possibile aggiungere commenti ai propri elementi Jump. Questa stringa ha un massimo di 1024 caratteri.
Procedura Jump (opzionale)	Nome codice di una procedura Jump. È possibile specificare una procedura Jump per gestire l'accesso a questo elemento Jump.
Procedura di sessione (opzionale)	Nome codice di una procedura di sessione. È possibile specificare una procedura di sessione per gestire le autorizzazioni disponibili su questo elemento Jump.

Collegamento RDP (Remote Desktop Protocol)

Campo	Descrizione
Nome Host	Nome host dell'endpoint a cui si accede con questo collegamento Jump.
Jumpoint	Nome codice del Jumpoint che l'endpoint utilizza per l'accesso.
Nome utente (opzionale)	Nome utente da utilizzare per l'accesso.
Dominio (opzionale)	Dominio su cui è presente l'endpoint.
Dimensione del display (opzionale)	Risoluzione per visualizzare il sistema remoto. Può essere **primaria** (predefinita, le dimensioni del monitor principale), **tutte** (le dimensioni di tutti i monitor combinati) o **XxY** (dove **X** e **Y** sono una combinazione di larghezza e altezza supportate, ad esempio **640x480**).
Qualità (opzionale)	Qualità per visualizzare il sistema remoto. Può essere **bassa** (scala di grigio a 2 bit per il consumo di banda più basso), **best_perf** (colore a 8 bit per prestazioni veloci), **perf_and_qual** (immagine a 16 bit per immagini e prestazioni di qualità media) o **best_qual** (risoluzione immagine più alta a 32 bit). Non è possibile modificarlo durante la sessione del protocollo RDP.
Sessione della console (opzionale)	**1**: Avvia una sessione della console. **0**: Avvia una nuova sessione (predefinita).
Ignora certificato non attendibile (opzionale)	**1**: Ignora le avvertenze del certificato. **0**: Mostra un'avvertenza se non è possibile verificare il certificato del server.
Gruppo Jump	Nome codice del team a cui si deve associare questo elemento Jump. ***Nota:*** *se si utilizza il metodo di importazione, non è possibile associare un elemento Jump a un gruppo Jump personale.*

Campo	Descrizione
Tag (opzionale)	È possibile organizzare gli elementi Jump in categorie aggiungendo un tag. Questa stringa ha un massimo di 1024 caratteri.
Commenti (opzionali)	È possibile aggiungere commenti ai propri elementi Jump. Questa stringa ha un massimo di 1024 caratteri.
Procedura Jump (opzionale)	Nome codice di una procedura Jump. È possibile specificare una procedura Jump per gestire l'accesso a questo elemento Jump.
Procedura di sessione (opzionale)	Nome codice di una procedura di sessione. È possibile specificare una procedura di sessione per gestire le autorizzazioni disponibili su questo elemento Jump.

Collegamento Shell Jump

Campo	Descrizione
Nome Host	Nome host dell'endpoint a cui si accede con questo collegamento Jump.
Jumpoint	Nome codice del Jumpoint che l'endpoint utilizza per l'accesso.
Nome utente (opzionale)	Nome utente da utilizzare per l'accesso.
Protocollo	Può essere **ssh** oppure **telnet**.
Porta (opzionale)	Numero di porta valido da **1** a **65535**. Il valore predefinito è **22** se il protocollo è **ssh** oppure **23** se il protocollo è **telnet**.
Tipo di terminale (opzionale)	Può essere **xterm** (predefinito) o **VT100**.
Keep-Alive (opzionale)	Numero di secondi tra ogni pacchetto inviato per tenere una sessione inattiva prima di terminare. Può essere qualsiasi numero da**0** a **300**. **0** disabilita il keep-alive (predefinito).
Gruppo Jump	Nome codice del team a cui si deve associare questo elemento Jump. ***Nota:*** *se si utilizza il metodo di importazione, non è possibile associare un elemento Jump a un gruppo Jump personale.*
Tag (opzionale)	È possibile organizzare gli elementi Jump in categorie aggiungendo un tag. Questa stringa ha un massimo di 1024 caratteri.
Commenti (opzionali)	È possibile aggiungere commenti ai propri elementi Jump. Questa stringa ha un massimo di 1024 caratteri.
Procedura Jump (opzionale)	Nome codice di una procedura Jump. È possibile specificare una procedura Jump per gestire l'accesso a questo elemento Jump.
Procedura di sessione (opzionale)	Nome codice di una procedura di sessione. È possibile specificare una procedura di sessione per gestire le autorizzazioni disponibili su questo elemento Jump.

Analizzatore endpoint: Report sulle porte aperte sugli endpoint

Configurazione analizzatore endpoint

Abilita analizzatore endpoint

Se l'opzione è abilitata, viene eseguita la scansione delle porte aperte una volta al giorno su tutti gli elementi Jump.

Porte TCP

Inserire le porte TCP da sottoporre a scansione. Inserire le porte da sottoporre a scansione separate da uno spazio o da una virgola oppure inserire un intervallo di porte separato da trattino tra il numero di porta minimo e il numero di porta massimo.

Porte UDP

Inserire le porte UDP da sottoporre a scansione. Inserire le porte da sottoporre a scansione separate da uno spazio o da una virgola oppure inserire un intervallo di porte separato da trattino tra il numero di porta minimo e il numero di porta massimo.

Report analizzatore endpoint

Tipo elemento Jump

Dal menu a discesa, selezionare il tipo di elemento Jump sul quale eseguire il report.

Jumpoint

È possibile restringere i risultati eseguendo un report soltanto sugli elementi Jump che si collegano mediante un Jumpoint selezionato.

Includi porte aperte già contrassegnate come previste

Restringere i risultati escludendo le porte già contrassegnate come previste.

Risultati dell'analizzatore endpoint

Visualizzare le porte aperte sugli endpoint specificati nella pagina precedente. È possibile impostare le porte come previsto per consentire di filtrarle per report futuri. È anche possibile impostare tutte le porte su impreviste.

Console di accesso

Impostazioni della console di accesso: Gestire impostazioni predefinite della console di accesso

Gestisci impostazioni della console di accesso

È possibile configurare le impostazioni della console di accesso per l'intera base dell'utente, applicando un'esperienza utente della console di accesso coerente e aumentando l'efficienza del team. È possibile forzare le impostazioni, consentire che le impostazioni vengano sovrascritte dall'utente o lasciare le impostazioni non gestite. Se si seleziona **Non gestito**, verrà visualizzata l'impostazione predefinita di Bomgar.

Ciascuna impostazione **Abilita** o **Disabilita** consente all'opzione della casella di controllo amministrativa di diventare un'impostazione predefinita. Le impostazioni forzate diventano effettive all'accesso successivo dell'utente e non consentono la configurazione nella console. Le impostazioni non forzate possono essere sovrascritte da un utente utilizzando la finestra delle impostazioni nella console di accesso. Non è possibile sovrascrivere un'impostazione forzata fino a quando un amministratore non deseleziona l'opzione della casella di controllo **Forzato** per quella impostazione nell'interfaccia amministrativa /login.

Scegliere le impostazioni che si vuole rendere predefinite per gli utenti e fare clic sul pulsante **Salva** nella parte inferiore della pagina.

Tenere presente che le impostazioni salvate hanno effetto soltanto dopo l'accesso alla console. Anche se le modifiche vengono salvate e applicate facendo clic sul pulsante **Applica ora** nella parte inferiore della pagina, come spiegato più avanti, l'utente non potrà utilizzare le nuove impostazioni fino all'accesso successivo.

Se, ad esempio, si desidera impostare le impostazioni predefinite per i nuovi utenti lasciando invariate le impostazioni esistenti, salvare le impostazioni gestite senza applicarle. Sarà possibile in tal modo consentire alle nuove console di accesso di eseguire l'accesso utilizzando le impostazioni predefinite gestite. Gli utenti esistenti troveranno le impostazioni forzate applicate all'accesso successivo, mentre le altre impostazioni resteranno invariate.

Impostazioni globali

Controllo ortografia abilitato

Dalla sezione **Impostazioni globali** è possibile abilitare o disabilitare il controllo ortografico per la chat. Il controllo ortografia è attualmente disponibile solo per l'inglese USA.

Barra laterale della sessione configurabile

Scegliere se si desidera visualizzare l'icona del menu di sessione, se la barra laterale può essere separata e se i widget sulla barra laterale di sessione possono essere riorganizzati e ridimensionati.

Avvisi :: Messaggi chat

Avvisi sonori - Emette un suono quando si riceve un messaggio chat

Selezionare per riprodurre un suono quando l'utente riceve un messaggio di chat. Se è attivato e non forzato o viene lasciato non gestito, l'utente può definire un suono personalizzato in formato WAV di dimensioni non superiori a 1 MB.

Avvisi visivi - L'icona dell'applicazione lampeggia quando si riceve un messaggio chat

Selezionare per far lampeggiare l'icona dell'applicazione quando l'utente riceve un messaggio di chat.

Mostra i messaggi di stato nelle finestre della chat del team

Selezionare se la chat del team deve includere i messaggi di stato, come ad esempio l'accesso o la disconnessione degli utenti oppure solo le chat inviate tra i membri del team.

Pop-up di notifiche

Code del team

Scegliere se un utente deve ricevere una notifica popup per i messaggi di chat ricevuti in una chat del team.

Sessioni di accesso

Scegliere se un utente deve ricevere una notifica popup per i messaggi di chat ricevuti in una sessione di accesso

Avvisi :: Coda Avvisi

Avvisi sonori - Emette un suono quando una sessione entra in una qualsiasi coda

Selezionare per riprodurre un suono quando una sessione entra in una delle code dell'utente.

Pop-up di notifiche

Le notifiche popup compariranno separate dalla console di accesso e nella parte superiore di altre finestre. Se la notifica popup è abilitata e non forzata o viene lasciata non gestita, l'utente sarà in grado di scegliere come ricevere le notifiche popup.

Coda personale - Sessioni condivise

Scegliere se un tecnico di supporto deve ricevere una notifica popup per le nuove sessioni in questa coda.

Code del team - Sessioni condivise

Scegliere se un tecnico di supporto deve ricevere una notifica popup per le nuove sessioni in questa coda.

Comportamento popup - Percorso e durata

Impostare il percorso e la durata predefiniti delle notifiche popup.

Sessioni di accesso :: Comportamento automatico

Richiedi automaticamente condivisione schermo

Scegliere se si desidera che le sessioni degli utenti debbano iniziare con la condivisione schermo.

Separa automaticamente

Scegliere se si vuole aprire le sessioni come schede nella console di accesso oppure separare automaticamente le sessioni in nuove finestre.

Eleva automaticamente tentativi di Jump della rete locale

Scegliere se il client dell'endpoint deve essere elevato automaticamente per l'esecuzione come servizio di sistema quando l'utente esegue un Jump sulla rete locale.

Ordina di innalzare i diritti se il desktop sicuro dell'endpoint è abilitato

Nei casi in cui gli utenti incontrino problemi perché è stata attivata la protezione del desktop, si può consentire agli utenti di elevare i propri diritti a livello amministrativo all'inizio della sessione.

Sessioni di accesso :: Strumenti

Condivisione schermo

Qualità predefinita

Impostare la qualità per una sessione con condivisione schermo.

Dimensionamento predefinito

Impostare le dimensioni per una sessione con condivisione schermo.

Inserisci automaticamente la modalità schermo intero all'avvio di condivisione schermo

All'avvio della condivisione schermo, l'utente può inserire automaticamente la modalità schermo intero.

Riduci automaticamente la barra laterale quando si utilizza la modalità schermo intero

Quando la sessione con condivisione schermo entra in modalità schermo intero, la barra di chat può ridursi automaticamente.

Shell di comando

Numero di righe della cronologia comandi disponibile

È possibile impostare il numero di righe da salvare nella cronologia della shell di comando. Il valore predefinito è 500 righe.

Salva

Fare clic su **Salva** per salvare tutte le impostazioni del profilo configurate. Viene visualizzato il messaggio di conferma **Il profilo delle impostazioni è stato salvato** nella parte superiore della finestra. Tutti gli utenti che accedono alla console di accesso dopo aver salvato il nuovo profilo riceveranno le nuove impostazioni come impostazioni predefinite.

Applica impostazioni della console di accesso gestite

Applica ora

Se si desidera inviare le impostazioni predefinite a tutta la base di utenti, fare clic su **Applica ora**. Nella parte superiore della finestra viene visualizzato il messaggio di conferma **Il profilo delle impostazioni è stato applicato**.

Dopo l'applicazione di nuove impostazioni alla base utenti, gli utenti riceveranno una finestra di avviso per la conferma al primo accesso alla console di accesso dopo aver applicato le impostazioni. Nella finestra di dialogo viene comunicato che le impostazioni sono cambiate e viene presentata l'opzione di aprire la finestra delle impostazioni della console di accesso per rivedere le modifiche o confermare la finestra di dialogo.

Collegamenti personalizzati: Aggiungere collegamenti URL alla console di accesso

Collegamenti personalizzati

Creare collegamenti ai siti ai quali gli utenti possono accedere durante le sessioni. Gli esempi potrebbero essere un collegamento a una knowledge base ricercabile, dando agli utenti la possibilità di cercare una soluzione al problema sul sistema dell'endpoint o una gestione delle relazioni con il cliente (Customer Relationship Management, CRM).

I collegamenti creati in questa sede diventano disponibili mediante il pulsante **Collegamenti** nella console di accesso.

Crea nuovo collegamento personalizzato, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Collegamenti personalizzati :: Aggiungi o Modifica

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

URL

Aggiungere gli URL ai quali questo collegamento personalizzato deve indirizzare. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Script preconfezionati: Creare script per la condivisione schermo e le sessioni shell di comando

Script preconfezionati

Creazione di script personalizzati da utilizzare nella condivisione schermo e nelle shell di comando in una sessione. Lo script sarà visualizzato nell'interfaccia della condivisione schermo e della shell di comando mentre viene eseguita. L'esecuzione di uno script nell'interfaccia della condivisione dello schermo consente di visualizzare lo script in esecuzione sullo schermo remoto.

Filtra in base a

Filtrare la visualizzazione selezionando una categoria o un team dall'elenco a discesa nella parte superiore della pagina.

Aggiungi nuovo script preconfezionato, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Script preconfezionato :: Aggiungi o Modifica

Nome script

Creare un nome univoco per consentire di identificare questo oggetto. Questo nome consente agli utenti di individuare lo script da eseguire.

Descrizione

Aggiungere una breve descrizione per riassumere lo scopo di questo oggetto. La descrizione è visualizzata sul prompt per confermare che l'utente desidera eseguire lo script selezionato.

Sequenza di comando

Scrivere la sequenza di comando. Gli script devono essere scritti in formato riga di comando, come quando si scrive un file batch o uno script della shell. Va notato che solo l'ultima riga dello script può essere interattiva; non si può eseguire un inserimento a metà testo.

All'interno dello script, indicare il file di risorse associato con **"%RESOURCE_FILE%"**, assicurandosi di mettere le virgolette. La sequenza di comando è soggetta a distinzione maiuscole/minuscole.

È possibile accedere alla directory provvisoria del file di risorse usando **"%RESOURCE_DIR%"**. Quando si esegue uno script con un file di risorse associato, questo file viene temporaneamente caricato nel computer del cliente.

Team

Selezionare il team che può utilizzare questo elemento.

Categorie

Selezionare la categoria sotto la quale sarà elencato l'elemento.

File di risorse

Si può selezionare un file di risorse da associare allo script.

Modalità elevazione

Selezionare se questo script deve essere disponibile per l'esecuzione solo in modalità elevata, solo in modalità non elevata o entrambe.

Categorie

Aggiungi categoria, Elimina

Creare una nuova categoria oppure rimuovere una categoria esistente.

Risorse

Caricamento

Aggiungere i file di risorse a cui si desidera accedere dagli script. È possibile caricare fino a 100 MB nella propria directory dei file di risorse.

Cancella

Rimuovere un file di risorse esistente.

Azioni speciali: Creazione azioni speciali personalizzate

Azioni speciali personalizzate

Creare le azioni speciali personalizzate per velocizzare i processi. Si possono creare azioni speciali per i sistemi Windows, Mac e Linux.

Aggiungi nuova azione speciale personalizzata, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Aggiungi o Modifica azione speciale

Nome azione

Creare un nome univoco per consentire di identificare questo oggetto. Durante una sessione, un utente può visualizzare questo nome nel menu a discesa delle azioni speciali.

Comando

Nel campo **Comando** immettere il percorso completo dell'applicazione da eseguire. Non utilizzare le virgolette; queste saranno aggiunte in caso di necessità. I sistemi Windows possono utilizzare le macro fornite. Se non è possibile individuare il comando nel sistema remoto, l'azione speciale personalizzata non viene visualizzata nell'elenco delle azioni speciali dell'utente.

Argomenti

Se il comando fornito accetta gli argomenti della riga di comando, successivamente sarà possibile immetterli. Gli argomenti possono utilizzare le virgolette, se necessario, e gli argomenti per i sistemi Windows possono utilizzare le macro fornite. Per la guida degli argomenti in Windows cercare "command line switches" nel sito msdn.microsoft.com.

Conferma

Se si seleziona la casella **Conferma**, agli utenti viene richiesto di confermare se desiderano eseguire questa azione speciale prima di eseguirla. In caso contrario, se si seleziona l'azione speciale personalizzata dal menu durante una sessione, l'azione speciale sarà eseguita subito.

Esegui elevati

Se si seleziona questa opzione, l'azione speciale viene visualizzata soltanto quando il client dell'endpoint viene eseguito in modalità elevata. Quando si esegue un'azione personalizzata in modalità elevata, viene richiesto di eseguirla come utente di sistema oppure di fornire le credenziali per un altro utente valido sul sistema remoto.

Impostazioni azioni speciali

Mostra azioni speciali incorporate

Per disabilitare le azioni speciali predefinite fornite da Bomgar, selezionare **Mostra azioni speciali incorporate**. In caso contrario, per abilitare soltanto le azioni speciali personalizzate deselezionare questa opzione.

Nota: *l'azione speciale* ***Protezione di Windows (Ctrl-Alt-Canc)*** *non può essere disabilitata. Se si disabilitano quindi le azioni speciali incorporate, non saranno disabilitate le azioni speciali predefinite per i dispositivi mobili.*

Sicurezza e Utenti

Utenti: Aggiungere autorizzazioni utente per un utente o admin

Account utenti

È possibile visualizzare dati su tutti gli utenti che hanno accesso al proprio dispositivo Bomgar, inclusi gli utenti locali e quelli che hanno accesso tramite l'integrazione di un fornitore di sicurezza.

Crea nuovo utente, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente. Non è possibile cancellare il proprio account.

Sincronizza

Sincronizzare gli utenti e i gruppi associati a un fornitore di sicurezza esterno. La sincronizzazione avviene automaticamente una volta al giorno. Facendo clic su questo pulsante viene forzata la sincronizzazione manuale.

Ricerca

È possibile cercare account utente in base al nome utente e al nome display.

Reimposta

Se un utente ha eseguito uno o più tentativi di accesso errati, fare clic sul pulsante **Reimposta** accanto al nome per reimpostare il numero su 0.

Utente :: Aggiungi o Modifica

Impostazioni utente

Nome utente

Identificatore esclusivo per il login.

Nome display

Nome dell'utente visualizzato nelle chat del team, nei report ecc.

Indirizzo email

Impostare un indirizzo e-mail per ricevere le e-mail di notifica, quali reimpostazione password o gli avvisi di modalità Disponibilità estesa.

Lingua preferita per email

Se in questo sito è abilitata più di una lingua, impostare la lingua da utilizzare per l'invio di e-mail.

Password

Password utilizzata assieme al nome utente per il login. La password può essere impostata su qualsiasi valore premesso che la stringa rientri nei limiti definiti nella procedura impostata nella pagina **/login > Gestione > Sicurezza**.

Invia password via email all'utente

Invia un'e-mail automatica all'utente con la nuova password. Se questa opzione è selezionata, l'utente deve reimpostare la propria password all'accesso successivo. Questa funzione richiede una valida configurazione SMTP per il dispositivo, da impostare nella pagina **/login > Gestione > Configurazione e-mail**.

Occorre reimpostare la password al prossimo login

Se questa opzione è selezionata, l'utente deve reimpostare la propria password all'accesso successivo.

La password scade il

Fa scadere la password dopo una determinata data o non la fa scadere mai.

Domanda di sicurezza e risposta di sicurezza

La domanda e la risposta di sicurezza consentono di resettare una password dimenticata dopo aver fornito la risposta esatta a questa domanda. Le password devono essere reimpostate solo se è selezionata l'opzione **Abilita reimpostazione password** nella pagina **Gestione > Sicurezza**. Gli amministratori non possono reimpostare le proprie password utilizzando la domanda di sicurezza.

Iscrizioni alla procedura di gruppo

Elenco delle procedure di gruppo alle quali appartiene l'utente con il collegamento alla pagina **Procedura di gruppo** o direttamente alle procedure di gruppo.

Appartenenza del team

Elenco dei team ai quali appartiene l'utente con il collegamento alla pagina **Team** o direttamente ai team.

Impostazioni account

Data ultima autenticazione

Data e ora dell'ultimo login dell'utente.

Codice di accesso e-mail

Abilita l'autenticazione a più fattori. Gli utenti ricevono una e-mail con un codice univoco di autenticazione ogni volta che accedono all'interfaccia amministrativa /login o alla console di accesso, desktop e mobile. Se per tre volte consecutive viene immesso il codice errato, è necessario immettere di nuovo le credenziali e ottenere un nuovo codice e-mail.

L'account scade il

Fa scadere l'account dopo una determinata data o non lo fa scadere mai.

Account disabilitato

Disattiva l'account in modo che l'utente non possa connettersi. La disattivazione NON cancella l'account.

Commenti

Inserire commenti per aiutare a identificare la finalità dell'oggetto.

Permessi

Amministratore

Concede all'utente pieni diritti amministrativi.

Consentito impostare password

Consente all'utente di impostare le password e di sbloccare gli account utente per gli utenti locali non amministrativi.

Consentito modificare i Jumpoint

Consente all'utente di creare o modificare i Jumpoints. Questa opzione non incide sulla capacità dell'utente di accedere a computer remoti tramite Jumpoint, che viene configurata per Jumpoint o procedura di gruppo.

Autorizzazioni report Sessione di accesso: Consentito visualizzare report delle sessioni di accesso

Consente a un utente di eseguire report sull'attività di sessione di accesso, visualizzando solo le sessioni di cui è il titolare principale, solo le sessioni in cui uno dei team era quello principale o uno dei suoi colleghi di team era il titolare di sessione principale oppure tutte le sessioni.

Consentito visualizzare registrazioni delle sessioni di accesso

Consente all'utente di vedere le registrazioni filmate di sessioni di condivisione schermo e della shell di comando.

Consentito usare report API

Consente di utilizzare le credenziali dell'utente da utilizzare per estrarre report XML tramite l'API.

Consentito usare il comando API

Consente di utilizzare le credenziali dell'utente per emettere comandi tramite l'API.

Consentito modificare team

Consente all'utente di creare o modificare i team.

Consentito modificare script preconfezionati

Consente all'utente di creare o modificare script preconfezionati da utilizzare nella condivisione schermo o in sessioni della shell di comando.

Consentito modificare i collegamenti personalizzati

Consente all'utente di creare o modificare i collegamenti personalizzati.

Autorizzazioni di accesso

Accesso

Consentito accedere agli endpoint

Consente all'utente di accedere alla console per eseguire sessioni. Se l'accesso all'endpoint è attivato, sono disponibili anche le opzioni di accesso all'endpoint.

Gestione sessione

Consentito condividere sessioni con i team a cui loro non appartengono

Consente all'utente di invitare un gruppo minore di utenti per condividere le sessioni, non solo i membri del proprio team. Se abbinata all'autorizzazione di disponibilità estesa, questa autorizzazione consente di espandere la propria capacità di condividere sessioni.

Consentito invitare utenti esterni

Consente all'utente di invitare un utente esterno a partecipare una tantum a una sessione.

Consentito abilitare la modalità Disponibilità estesa

Consente di ricevere e-mail di invito da altri utenti che chiedono di condividere una sessione quando non sono connessi alla console di accesso.

Consentito modificare la chiave esterna

Consente all'utente di modificare la chiave esterna nel pannello Informazioni sessione di una sessione nell'ambito della console di accesso.

Condivisione schermo da utente a utente

Consentito mostrare lo schermo ad altri utenti

Consente all'utente di condividere il proprio schermo con un altro utente senza che l'utente ricevente debba partecipare a una sessione. Questa opzione è disponibile anche se l'utente non è nella sessione.

Consentito dare il controllo quando si mostra lo schermo ad altri utenti

Consente all'utente di condividere il proprio schermo per dare il controllo di tastiera e mouse all'utente che visualizza lo schermo.

Tecnologia Jump

Metodi Jump consentiti: Consentito avviare sessioni da Jump Clients che utilizzano uno dei seguenti metodi Jump

Consente all'utente di eseguire il Jump a computer tramite **Jump Client**, **Jump locale sulla rete locale**, **Jump remoto mediante un Jumpoint**, **RDP mediante un Jumpoint** e/o **Shell Jump mediante un Jumpoint**.

Autorizzazioni elemento Jump: Consentito avviare sessioni da tutti gli elementi Jump del sistema

Consente all'utente di eseguire il Jump a computer remoti su tutti i gruppi Jump del team.

Autorizzato a distribuire, rimuovere e modificare elementi Jump nei seguenti gruppi Jump

Autorizza l'utente a vincolare sessioni, impostare gruppi e aggiungere commenti a elementi Jump solo per il gruppo Jump personale, per i team e i gruppi Jump dei membri del team oppure per tutti i gruppi Jump, compresi quelli distribuiti a team a cui l'utente non appartiene e a un qualsiasi Gruppo Jump personale di un utente.

Consentito modificare le procedure di sessione associate agli elementi Jump

Consente all'utente di impostare la procedura di sessione che deve utilizzare un elemento Jump. La modifica della procedura di sessione può influenzare le autorizzazioni consentite nella sessione.

Autorizzazioni sessione

Impostare le regole di prompt e di autorizzazione da applicare alle sessioni di questo utente. Scegliere una procedura di sessione esistente o definire le autorizzazioni personalizzate per questo utente. Se **non definita**, sarà utilizzata la procedura globale predefinita. Queste autorizzazioni possono essere sovrascritte da una procedura superiore.

Descrizione

Visualizza la descrizione di una procedura di autorizzazione di sessione predefinita.

Condivisione schermo

Condivisione schermo

Consente all'utente di visualizzare o controllare lo schermo remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Limitazioni di condivisione applicazione

Limitare l'accesso a determinate applicazioni sul sistema remoto con l'opzione **Consenti soltanto gli eseguibili elencati** oppure **Rifiuta soltanto gli eseguibili elencati**. È anche possibile scegliere di consentire o rifiutare l'accesso al desktop.

Nota: *questa funzione si applica soltanto ai sistemi operativi Windows e Linux e non comprende le sessioni Remote Desktop Protocol (RDP).*

Aggiungi nuovo(i) eseguibile(i)

Se vengono applicate le restrizioni sulla condivisione delle applicazioni, viene visualizzato un pulsante **Aggiungi nuovo(i) eseguibile(i)**. Facendo clic su questo pulsante si apre una finestra che consente di specificare i file eseguibili per negare o consentire, a seconda dei propri obiettivi.

Dopo aver aggiunto i file eseguibili, una o due tabelle mostrano i nomi dei file o gli hash selezionati per la restrizione. Un campo commenti modificabile consente note amministrative.

Inserire i nomi file o gli hash SHA-256, uno per riga

Quando si limitano gli eseguibili, inserire manualmente i nomi dei file eseguibili o gli hash che si desidera consentire o negare. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Cerca uno o più file

Quando si limitano gli eseguibili, selezionare questa opzione per navigare nel sistema e scegliere i file eseguibili per ricavare automaticamente i nomi o gli hash. Se si selezionano i file dalla piattaforma locale e dal sistema in questo modo, accertarsi che i file siano effettivamente file eseguibili. Non viene eseguita alcuna verifica a livello di browser.

Scegliere **Utilizzare il nome file** o **Utilizzare l'hash del file** in modo che il browser ricavi automaticamente i nomi o gli hash dei file eseguibili. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Nota: *questa opzione è disponibile solo nei browser moderni non in quelli precedenti.*

Limitazioni dell'endpoint consentite

Consente di impostare se l'utente può sospendere l'input del mouse e della tastiera del sistema remoto. L'utente può anche impedire al desktop remoto di essere visualizzato.

Consentito accedere utilizzando le credenziali di un gestore delle credenziali di endpoint

Abilitare la connessione di un utente al proprio Manager credenziali endpoint per utilizzare le credenziali dal proprio archivio password o insieme di credenziali esistenti.

L'utilizzo del Manager credenziali endpoint richiede un accordo separato sui servizi con Bomgar. Dopo aver stipulato l'accordo, è possibile scaricare il middleware richiesto dal centro self-service Bomgar.

> ***Nota:*** *prima della versione 15.2, questa funzione era disponibile soltanto nelle sessioni avviate da Jump Client elevati su Windows®. A partire dalla versione 15.2, è possibile utilizzare un Manager credenziali endpoint nelle sessioni Jump remote, nelle sessioni Microsoft® Remote Desktop Protocol e nelle sessioni Shell Jump. è anche possibile utilizzare questa funzione con l'azione speciale Esegui come in una sessione di condivisione schermo su un sistema Windows®.*

Annotazioni

Consente all'utente di usare gli strumenti di annotazione per disegnare sullo schermo dell'utente remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Trasferimento file

Trasferimento file

Consente all'utente di caricare file nel sistema remoto, scaricare file dal sistema remoto o entrambe le operazioni. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Percorsi accessibili sul file system dell'endpoint

Consente all'utente di trasferire file a o da qualsiasi directory nel sistema remoto oppure solo a o da determinate directory.

Percorsi accessibili sul file system dell'utente

Consente all'utente di trasferire file a o da qualsiasi directory nel proprio sistema locale oppure solo a o da determinate directory.

Shell di comando

Shell di comando

Consente all'utente di inserire comandi nel computer remoto tramite un'interfaccia virtuale della riga di comando. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Informazioni del sistema

Informazioni del sistema

Consente all'utente di vedere le informazioni di sistema sul computer remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Consentito utilizzare le azioni sulle informazioni di sistema

Consente all'utente di interagire con i processi e i programmi del sistema remoto senza richiedere la condivisione schermo. Arresto dei processi; avvio, arresto, pausa, ripresa e riavvio dei servizi e disinstallazione dei programmi.

Accesso al registro di sistema

Accesso al registro di sistema

Consente all'utente di interagire con il registro del sistema remoto Windows senza richiedere la condivisione schermo. Visualizzazione, aggiunta, eliminazione e modifica delle chiavi, ricerca e importazione/esportazione delle chiavi.

Altri strumenti

Script preconfezionati

Consente all'utente di eseguire script preconfezionati, creati per i suoi team. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Elevazione

Consente all'utente di tentare di elevare il client dell'endpoint per funzionare con diritti amministrativi nel sistema remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Programma di login

Accesso dell'utente limitato al programma seguente

Impostare una programmazione per definire quando gli utenti possono accedere alla console. Impostare il fuso orario da utilizzare per la programmazione e aggiungere una o più voci di programmazione. Per ciascuna voce, immettere il giorno e l'ora di inizio e il giorno e l'ora di fine.

Se, ad esempio, è stato impostato l'inizio alle ore 8.00 e la fine alle ore 17.00, un utente può accedere in qualsiasi momento durante questa finestra temporale, ma può continuare a lavorare oltre il limite di fine impostato. Tuttavia non potrà riconnettersi dopo le 17.00.

Forza disconnessione quando il programma non consente il login

Se è richiesto il controllo degli accessi, selezionare questa opzione. In tal modo l'utente viene disconnesso all'ora di fine pianificata. In questo caso, l'utente inizia a ricevere notifiche ripetute 15 minuti prima della disconnessione. Quando un utente

viene disconnesso, tutte le sessioni pertinenti seguiranno le regole di fallback della sessione.

Report sull'account utente

Esportare le informazioni dettagliate sugli utenti a scopo di controllo. Raccogliere informazioni dettagliate per tutti gli utenti, gli utenti di uno specifico fornitore di protezione o soltanto degli utenti locali. Le informazioni raccolte comprendono i dati visualizzati sotto il pulsante "Mostra dettagli", la procedura di gruppo, le appartenenze al team e le autorizzazioni.

Account utenti per reimpostazione password: Consenti agli utenti di gestire le password

Account utenti

Gli amministratori possono delegare, mediante autorizzazione dell'utente, il compito di reimpostare le password degli utenti locali e gli account utente bloccati per gli utenti privilegiati senza dover inoltre concedere autorizzazioni di amministratore complete. Gli utenti locali possono continuare a reimpostare le proprie password.

***Nota:** gli amministratori con l'autorizzazione **Consentito impostare password** non vedranno alcuna differenza nell'interfaccia utente.*

Quando un utente con privilegi non amministratore entra nella pagina **Utenti e sicurezza > Utenti** nell'interfaccia amministrativa /login, avrà una vista limitata **Utenti** contenente link **Cambia password** per gli utenti non amministratori. L'utente privilegiato non sarà in grado di modificare o eliminare gli account utente. Gli utenti privilegiati non possono reimpostare le password degli amministratori né le password degli utenti che forniscono la protezione.

Ricerca

È possibile cercare account utente in base al nome utente e al nome display.

Reimposta

Se un utente ha eseguito uno o più tentativi di accesso errati, fare clic sul pulsante **Reimposta** accanto al nome per reimpostare il numero su 0.

Cambia Password

Consente di cambiare la password per un utente non amministrativo.

Utente :: Cambia Password

Nome utente

Identificatore esclusivo per il login. Questo campo non può essere modificato.

Nomi visualizzati

Nome dell'utente visualizzato nelle chat del team, nei report ecc. Questo campo non può essere modificato.

Indirizzo email

L'indirizzo e-mail per ricevere le e-mail di notifica, quali reimpostazione password o gli avvisi di modalità Disponibilità estesa. Questo campo non può essere modificato.

Commenti

Commenti sull'account. Questo campo non può essere modificato.

Password

La nuova password da assegnare a questo account utente. La password può essere impostata su qualsiasi valore premesso che la stringa rientri nei limiti definiti nella procedura impostata nella pagina **/login > Gestione > Sicurezza**.

Invia password via email all'utente

Invia un'e-mail automatica all'utente con la nuova password. Se questa opzione è selezionata, l'utente deve reimpostare la propria password all'accesso successivo. Questa funzione richiede una valida configurazione SMTP per il dispositivo, da impostare nella pagina **/login > Gestione > Configurazione e-mail**.

Occorre reimpostare la password al prossimo login

Se questa opzione è selezionata, l'utente deve reimpostare la propria password all'accesso successivo.

Invito di accesso: Creare profili per invitare alle sessioni gli utenti esterni

E-mail di invito di accesso

Con la funzione Invito di accesso, un utente con privilegi può invitare un utente esterno a partecipare una tantum a una sessione. Nell'estendere l'invito, l'utente deve selezionare un profilo di sicurezza per determinare il livello dei privilegi da concedere all'utente esterno. I profili di sicurezza invito di accesso sono configurati come procedure di sessione nella pagina **Utenti e sicurezza > Procedure di sessione** e devono essere abilitati per l'uso degli inviti di accesso.

L'invito e-mail viene inviato agli utenti esterni invitati a partecipare a una sessione.

Oggetto

Personalizzare l'oggetto di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Testo

Personalizzare il corpo di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Fornitori di sicurezza: Abilitare LDAP, Active Directory, RADIUS e gli accessi Kerberos

Fornitori di sicurezza

È possibile configurare il proprio dispositivo Bomgar per autenticare gli utenti rispetto a server esistenti LDAP, RADIUS o Kerberos nonché per assegnare privilegi basati sulle preesistenti impostazioni di gerarchia e di gruppo già specificate nei server. Kerberos attiva il meccanismo di accesso Single Sign-On mentre RSA e altri meccanismi di autenticazione multifattore tramite RADIUS offrono un ulteriore livello di sicurezza.

Crea provider

Crea una nuova configurazione del fornitore della sicurezza. Dal menu a discesa selezionare un fornitore LDAP, un fornitore RADIUS o un fornitore Kerberos.

Visualizza log

Visualizza la cronologia dello stato per una connessione del fornitore di sicurezza.

Sincronizzazione

Sincronizzare gli utenti e i gruppi associati a un fornitore di sicurezza esterno. La sincronizzazione avviene automaticamente una volta al giorno. Facendo clic su questo pulsante viene forzata la sincronizzazione manuale.

Disabilita

Disabilitare la connessione del fornitore di sicurezza. Questo risulta utile per la manutenzione programmata quando si desidera che il server sia offline ma non eliminato.

Modifica, Elimina

Modifica oppure rimuove un oggetto esistente.

Crea copia

Crea una copia della configurazione di un fornitore della sicurezza esistente. Questo verrà aggiunto come fornitore della sicurezza di livello superiore e non come parte di un cluster.

Duplica nodo

Crea una copia della configurazione di un fornitore della sicurezza nel cluster esistente. Questo verrà aggiunto come nuovo nodo nello stesso cluster.

Upgrade a cluster

Aggiorna un fornitore della sicurezza a un cluster di fornitore della sicurezza. Per aggiungere più fornitori della sicurezza a questo cluster, copiare un nodo esistente.

Modifica ordine

Fare clic su questo pulsante per trascinare i fornitori della sicurezza per l'impostazione della priorità. È possibile trascinare server in un gruppi e anche i gruppo stessi. Per rendere effettive le modifiche dell'ordine di priorità, cliccare su **Salva ordine**.

Fornitori di sicurezza :: Modifica - LDAP

Impostazioni generali

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

Abilitato: Questo provider è abilitato

Se questa opzione è selezionata, il dispositivo Bomgar può cercare il fornitore di sicurezza quando un utente tenta l'accesso. Se l'opzione non è selezionata, il fornitore non sarà cercato.

Nomi utente visualizzati: Mantieni il nome del display sincronizzato con il sistema remoto

Questi valori stabiliscono i campi da utilizzare come nomi visualizzati privato e pubblico dell'utente.

Sincronizzazione: Abilita cache oggetti LDAP

Se questa opzione è selezionata, gli oggetti visibili al dispositivo vengono collocati nella cache e sincronizzati di notte, o manualmente, se desiderato. Quando si utilizza questa opzione, vengono eseguire meno connessioni al server LDAP per scopi amministrativi che quindi possono aumentare la velocità e l'efficienza.

Se non è selezionata, le modifiche apportate al server LDAP sono subito disponibili senza dover sincronizzare. Tuttavia, quando si apportano modifiche alle procedure utente dall'interfaccia amministrativa, si possono verificare diverse connessioni LDAP di breve durata.

Per i provider che hanno già abilitato l'impostazione di sincronizzazione, disabilitare o deselezionare l'opzione di sincronizzazione può comportare l'eliminazione di tutti i record presenti nella cache che non sono in uso al momento.

Impostazioni di autorizzazione

Ricerca gruppi

Scegliere di utilizzare questo fornitore di sicurezza solo per l'autenticazione utente, solo per le ricerche di gruppo o per entrambi.

Procedura di gruppo predefinito *(visibile solo se è consentita l'autenticazione utente)*

Ogni utente autenticabile rispetto a un server esterno deve essere membro di almeno una procedura di gruppo per autenticarsi sul dispositivo Bomgar e deve accedere all'interfaccia /login o alla console di accesso. È possibile selezionare una procedura di gruppo predefinito da applicare a tutti gli utenti che sono autorizzati ad autenticarsi su un server configurato.

Tenere presente che se viene definita una procedura predefinita, ogni utente che si autentica su questo server avrà accesso potenzialmente al livello di questa procedura predefinita. Si consiglia quindi di impostare i valori predefiniti della procedura con i privilegi minimi per impedire agli utenti di ottenere le autorizzazioni che non si desidera fargli avere.

***Nota:** se un utente è in una procedura di gruppo predefinito e viene quindi specificamente aggiunto a un'altra procedura di gruppo predefinito, le impostazioni per la procedura specifica avranno sempre la precedenza sulle impostazioni predefinite anche se la procedura specifica ha una priorità inferiore rispetto al valore predefinito e anche se le impostazioni della procedura predefinita sono impostate per non consentire la sovrascrittura.*

Impostazioni di connessione

Nome Host

Immettere il nome host del server che ospita l'archivio della directory esterno.

***Nota:** se si utilizza **LDAPS** o **LDAP con TLS**, il nome host deve corrispondere al nome host utilizzato nel nome oggetto del certificato SSL pubblico del server LDAP o nel componente DNS del nome dell'oggetto alternativo.*

Porta

Specificare la porta del server LDAP. In genere è la porta **389** per LDAP o **636** per LDAPS. Bomgar inoltre supporta il catalogo globale sulla porta **3268** per LDAP o **3269** per LDAPS.

Cifratura

Selezionare il tipo di crittografia da utilizzare quando si comunica con il server LDAP. Per motivi di sicurezza si consiglia **LDAPS** o **LDAP con TLS**.

***Nota:** LDAP regolare invia e riceve i dati in chiaro dal server LDAP, esponendo potenzialmente le informazioni sensibili relative all'account utente al packet sniffing. LDAPS e LDAP con TLS criptano i dati utente quando vengono trasferiti, rendendo questi metodi consigliati su LDAP regolare. LDAP con TLS utilizza la funzione StartTLS per avviare una connessione LDAP in chiaro, ma poi la eleva per una connessione crittografata. LDAPS avvia la connessione tramite una connessione criptata senza inviare alcun dato in chiaro.*

Se si seleziona **LDAP** o **LDAP con TLS**, è necessario caricare il certificato SSL principale utilizzato dal server LDAP. Questo è necessario per assicurare la validità del server e la sicurezza dei dati. Il certificato principale deve essere in formato PEM.

***Nota:** se il nome dell'oggetto del certificato SSL pubblico del server LDAP o il componente DNS del nome dell'oggetto alternativo non corrisponde al valore nel campo **nome host**, il fornitore sarà trattato come non raggiungibile. È tuttavia possibile utilizzare un certificato con i caratteri jolly per certificare più domini secondari dello stesso sito. Ad esempio, un certificato per ***.example.com** certifica **access.example.com** e **remote.example.com**.*

Credenziali BIND

Specificare un nome utente e una password da associare al dispositivo Bomgar e cercare l'archivio della directory LDAP.

Se il server supporta binding anonimi, è possibile scegliere di associare senza specificare un nome utente e una password. Il binding anonimo non è considerato sicuro ed è disabilitato per impostazione predefinita nella maggior parte dei server LDAP.

Metodo di connessione

Se si utilizza un archivio directory esterno sulla stessa LAN del dispositivo Bomgar, i due sistemi possono comunicare direttamente, nel qual caso è possibile lasciare deselezionata l'opzione **Proxy del dispositivo mediante agente di connessione** e andare avanti.

Se i due sistemi non sono in grado di comunicare direttamente, ad esempio nel caso in cui il server di directory esterno si trova dietro il firewall, è necessario utilizzare un agente di collegamento. Scaricando l'agente di collegamento Win32 si attiva il server di directory e il dispositivo Bomgar per comunicare tramite SSL crittografato, per la connessione in uscita, senza alcuna configurazione del firewall. L'agente di connessione può essere scaricato sul server di directory o su un server separato sulla stessa rete del server di directory (consigliato).

Nel caso precedente, selezionare **Proxy del dispositivo mediante agente di connessione**. Creare una **Password agente di connessione** da utilizzare nel processo di installazione dell'agente di connessione. Quindi fare clic su **Scarica l'agente di connessione**, eseguire il programma di installazione e seguire la guida all'installazione. Durante l'installazione verrà richiesto di inserire il nome del fornitore di sicurezza e la password per il nome utente creato in precedenza.

Tipo di directory

Per facilitare la configurazione della connessione di rete tra il dispositivo Bomgar e il fornitore di sicurezza, è possibile selezionare un tipo di directory come modello. Questa pre-popola i campi di configurazione di seguito con i dati standard, ma deve essere modificata per corrispondere alla configurazione specifica del fornitore di sicurezza. LDAP Active Directory è il tipo di server più comune, anche se è possibile configurare Bomgar per comunicare con la maggior parte dei tipi di fornitori di sicurezza.

Impostazioni cluster *(visibile solo per i cluster)*

Algoritmo della selezione dei membri

Selezionare il metodo per cercare i nodi in questo cluster.

Dall'alto verso il basso prima tenta il server con la priorità più alta nel cluster. Se quel server non è disponibile o l'account non viene trovato, viene tentato il server successivo con la priorità più alta. La ricerca prosegue verso il basso con l'elenco di server nel cluster fino a quando l'account viene trovato o si stabilisce che l'account non esiste in nessuno dei server specificati e disponibili.

Round-robin è progettato per bilanciare il carico tra più server. L'algoritmo sceglie a caso il server da provare per primo. Se quel server non è disponibile o l'account non viene trovato, viene tentato un altro a caso. La ricerca continua a caso tra i server rimanenti nel cluster fino a quando l'account viene trovato o si stabilisce che l'account non esiste in nessuno dei server specificati e disponibili.

Riprova ritardo

Impostare il tempo di attesa dopo il quale un membro del cluster non è disponibile prima di provare ancora una volta quel membro del cluster.

Impostazioni schema utente

Sovrascrivi i valori del cluster *(visibile solo per i nodi cluster)*

Se questa opzione è selezionata, il nodo cluster utilizzerà le stesse impostazioni dello schema del cluster. Se non è selezionata, sarà possibile modificare le impostazioni dello schema seguenti.

DN base di ricerca

Stabilire il livello nella gerarchia della directory, specificato con un nome completo, dove il dispositivo Bomgar deve iniziare la ricerca degli utenti. A seconda delle dimensioni dell'archivio della directory e gli utenti che richiedono gli account Bomgar, è possibile migliorare le prestazioni individuando l'unità organizzativa nell'archivio della directory che richiede l'accesso. Se non si è sicuri o se gli utenti appartengono a più unità organizzative, specificare il nome completo radice dell'archivio della directory.

Query utente

Specificare le informazioni della query che il dispositivo Bomgar deve utilizzare per localizzare un utente LDAP quando l'utente tenta di accedere. Il campo **Query utente** accetta una query standard LDAP (RFC 2254 - rappresentazione stringa dei filtri di ricerca LDAP). È possibile modificare la stringa della query per personalizzare l'accesso degli utenti e i metodi accettati dei nomi utente. Per specificare il valore nella stringa da utilizzare come nome, sostituire il valore con *.

Sfoglia query

Sfoglia query riguarda la visualizzazione dei risultati durante la navigazione attraverso le procedure di gruppo. Vengono filtrati i risultati per visualizzare solo certi risultati nel menu a discesa per la selezione dei membri quando si aggiungono i membri a una procedura di gruppo.

Classi oggetti

Specificare classi di oggetti validi per un utente all'interno dell'archivio directory. Verranno autenticati solo gli utenti che possiedono una o più di queste classi di oggetti. Queste classi di oggetti sono utilizzate anche con i nomi degli attributi seguenti per indicare al dispositivo Bomgar lo schema che il server LDAP utilizza per identificare gli utenti. È possibile immettere più classi oggetti, uno per riga.

Nomi attributo

Specificare i campi da utilizzare per un ID univoco dell'utente e il nome utente.

ID univoco

Questo campo richiede un identificatore unico per l'oggetto. Mentre il nome distinto può servire come questo ID, il nome distinto di un utente può cambiare frequentemente nel corso della vita di un utente, come ad esempio con un cambio di nome o di posizione o con la ridenominazione dell'archivio LDAP. Pertanto, la maggior parte dei server LDAP incorporano qualche campo che è unico per ogni oggetto e non cambia per tutta la vita dell'utente. Se si utilizza il nome distinto come ID univoco e le modifiche di nome distinto di un utente, questo utente sarà visto come un nuovo utente e tutte le modifiche eseguite in modo specifico sul singolo account utente Bomgar non saranno applicate al nuovo utente. Se il server LDAP non incorpora un identificatore univoco, utilizzare un campo che ha meno probabilità di avere una voce identica per un altro utente.

Utilizzare lo stesso attributo per nomi visualizzati pubblici e privati

Se questa opzione è selezionata, è possibile specificare valori separati per i nomi display privati e pubblici dell'utente.

Nomi visualizzati

Questi valori stabiliscono i campi da utilizzare come nomi visualizzati privato e pubblico dell'utente.

Impostazioni schema gruppo *(visibile solo se si eseguono ricerche di gruppo)*

DN base di ricerca

Stabilire il livello nella gerarchia della directory, specificato con un nome completo, dove il dispositivo Bomgar deve iniziare la ricerca dei gruppi. A seconda delle dimensioni dell'archivio della directory e dei gruppi che richiedono l'accesso al dispositivo Bomgar, è possibile migliorare le prestazioni individuando l'unità organizzativa nell'archivio della directory che richiede l'accesso. Se non si è sicuri o se i gruppi appartengono a più unità organizzative, specificare il nome completo radice dell'archivio della directory.

Sfoglia query

Sfoglia query riguarda la visualizzazione dei risultati durante la navigazione attraverso le procedure di gruppo. Vengono filtrati i risultati per visualizzare solo certi risultati nel menu a discesa per la selezione dei membri quando si aggiungono i membri a una procedura di gruppo.

Classi oggetti

Specificare classi di oggetti validi per un gruppo all'interno dell'archivio directory. Verranno restituiti solo i gruppi che possiedono una o più di queste classi di oggetti. Queste classi di oggetti sono utilizzate anche con i nomi degli attributi seguenti per indicare al dispositivo Bomgar lo schema che il server LDAP utilizza per identificare i gruppi. È possibile immettere più classi oggetti di gruppo, uno per riga.

Nomi attributo

Specificare i campi da utilizzare per un ID univoco del gruppo e il nome visualizzato.

ID univoco

Questo campo richiede un identificatore unico per l'oggetto. Mentre il nome distinto può servire come questo ID, il nome distinto di un gruppo può cambiare frequentemente nel corso della vita di un gruppo, come ad esempio con un cambio di posizione o con la ridenominazione dell'archivio LDAP. Pertanto, la maggior parte dei server LDAP incorporano qualche campo che è unico per ogni oggetto e non cambia per tutta la vita del gruppo. Se si utilizza il nome distinto come ID univoco e il nome distinto di un gruppo cambia, questo gruppo sarà visto come un nuovo gruppo e tutte le procedure di gruppo definite per quel gruppo non saranno applicate al nuovo gruppo. Se il server LDAP non incorpora un identificatore univoco, utilizzare un campo che ha meno probabilità di avere una voce identica per un altro gruppo.

Nome display

Questo valore stabilisce il campo da utilizzare come nome visualizzato del gruppo.

Rapporti da utente a gruppo

Questo campo richiede una query per stabilire quali utenti appartengono a determinati gruppi o, al contrario, quali gruppi contengono determinati utenti.

Esegui una ricerca ricorsiva per gruppi

È possibile scegliere di eseguire una ricerca ricorsiva per gruppi. Verrà eseguita una query per un utente, quindi delle query per tutti i gruppi a cui l'utente appartiene, quindi delle query per tutti i gruppi a cui appartengono quei gruppi e così via, fino a quando sono stati trovati tutti i gruppi possibili associati a tale utente.

L'esecuzione di una ricerca ricorsiva può avere un impatto significativo sulle prestazioni poiché il server continuerà a emettere le query fino a quando non ha trovato le informazioni su tutti i gruppi. Se impiega troppo tempo, l'utente potrebbe non essere in grado di eseguire il login.

Una ricerca non ricorsiva emetterà una sola query per utente. Se il server LDAP ha un campo speciale che contiene tutti i gruppi ai quali appartiene l'utente, la ricerca ricorsiva non è necessaria. La ricerca ricorsiva non è inoltre necessaria se la struttura della directory non gestisce i membri dei gruppi.

Impostazioni test

Nome utente e password

Inserire nome utente e password per un account esistente sul server che si sta testando. Questo account deve corrispondere ai criteri di accesso specificati nella configurazione precedente.

Cercare di ottenere gli attributi utente e le iscrizioni di gruppo se le credenziali sono accettate

Se questa opzione è selezionata, il test delle credenziali corretto tenta di verificare anche gli attributi utente e la ricerca del gruppo. Tenere presente che per il test corretto queste funzioni devono essere supportate e configurate nel fornitore di sicurezza.

Avvia test

Se il server è correttamente configurato e sono stati inseriti un nome utente e password di test validi, si riceverà un messaggio di conferma. In caso contrario, verrà visualizzato un messaggio di errore e un registro che consente di eseguire il debug del problema.

Fornitori di sicurezza :: Modifica - RADIUS

Impostazioni generali

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

Abilitato: Questo provider è abilitato

Se questa opzione è selezionata, il dispositivo Bomgar può cercare il fornitore di sicurezza quando un utente tenta l'accesso. Se l'opzione non è selezionata, il fornitore non sarà cercato.

Nomi visualizzati: Mantieni il nome del display sincronizzato con il sistema remoto

Questi valori stabiliscono i campi da utilizzare come nomi visualizzati privato e pubblico dell'utente.

Impostazioni di autorizzazione

Consentire soltanto i seguenti utenti

È possibile scegliere di concedere l'accesso solo a determinati utenti sul server RADIUS. Immettere ogni nome utente separato da un'interruzione di riga. Una volta immessi, questi utenti saranno disponibili nella finestra di dialogo **Aggiungi membro della procedura** quando si modificano le procedure di gruppo nella pagina **/login > Utenti e sicurezza > Procedure di gruppo**.

Se si lascia vuoto questo campo, saranno autorizzati tutti gli utenti che eseguono l'autenticazione sul server RADIUS; se si consente tutto, è necessario specificare anche una procedura di gruppo predefinito.

Ricerca del gruppo LDAP

Se si desidera che gli utenti su questo fornitore di sicurezza siano associati ai loro gruppi in un server LDAP separato, scegliere uno o più server di gruppo LDAP da utilizzare per la ricerca del gruppo.

Procedura di gruppo predefinito

Ogni utente autenticabile rispetto a un server esterno deve essere membro di almeno una procedura di gruppo per autenticarsi sul dispositivo Bomgar e deve accedere all'interfaccia /login o alla console di accesso. È possibile selezionare una procedura di gruppo predefinito da applicare a tutti gli utenti che sono autorizzati ad autenticarsi su un server configurato.

Impostazioni di connessione

Nome Host

Immettere il nome host del server che ospita l'archivio della directory esterno.

Porta

Specificare la porta di autenticazione per il server RADIUS. In genere è la porta **1812**.

Metodo di connessione

Se si utilizza un archivio directory esterno sulla stessa LAN del dispositivo Bomgar, i due sistemi possono comunicare direttamente, nel qual caso è possibile lasciare deselezionata l'opzione **Proxy del dispositivo mediante agente di connessione** e andare avanti.

Se i due sistemi non sono in grado di comunicare direttamente, ad esempio nel caso in cui il server di directory esterno si trova dietro il firewall, è necessario utilizzare un agente di collegamento. Scaricando l'agente di collegamento Win32 si attiva il server di directory e il dispositivo Bomgar per comunicare tramite SSL crittografato, per la connessione in uscita, senza alcuna configurazione del firewall. L'agente di connessione può essere scaricato sul server di directory o su un server separato sulla stessa rete del server di directory (consigliato).

Nel caso precedente, selezionare **Proxy del dispositivo mediante agente di connessione**. Creare una **Password agente di connessione** da utilizzare nel processo di installazione dell'agente di connessione. Quindi fare clic su **Scarica l'agente di connessione**, eseguire il programma di installazione e seguire la guida all'installazione. Durante l'installazione verrà richiesto di inserire il nome del fornitore di sicurezza e la password per il nome utente creato in precedenza.

Informazione segreta

Fornire un nuovo segreto condiviso in modo che il dispositivo Bomgar e il server RADIUS possano comunicare.

Time-out (secondi)

Impostare il tempo massimo di attesa di una risposta dal server. Tenere presente che se la risposta è **Risposta-Accetta** o **Risposta-Sfida**, il server RADIUS attenderà tutto il tempo specificato prima di autenticare l'account. Si consiglia quindi di mantenere questo valore il più basso possibile secondo le impostazioni della rete. Il valore ideale è di 3-5 secondi con un valore massimo di tre minuti.

Impostazioni cluster *(visibile solo per i cluster)*

Algoritmo della selezione dei membri

Selezionare il metodo per cercare i nodi in questo cluster.

Dall'alto verso il basso prima tenta il server con la priorità più alta nel cluster. Se quel server non è disponibile o l'account non viene trovato, viene tentato il server successivo con la priorità più alta. La ricerca prosegue verso il basso con l'elenco di server nel cluster fino a quando l'account viene trovato o si stabilisce che l'account non esiste in nessuno dei server specificati e disponibili.

Round-robin è progettato per bilanciare il carico tra più server. L'algoritmo sceglie a caso il server da provare per primo. Se quel server non è disponibile o l'account non viene trovato, viene tentato un altro a caso. La ricerca continua a caso tra i server rimanenti nel cluster fino a quando l'account viene trovato o si stabilisce che l'account non esiste in nessuno dei server specificati e disponibili.

Riprova ritardo

Impostare il tempo di attesa dopo il quale un membro del cluster non è disponibile prima di provare ancora una volta quel membro del cluster.

Impostazioni test

Nome utente e password

Inserire nome utente e password per un account esistente sul server che si sta testando. Questo account deve corrispondere ai criteri di accesso specificati nella configurazione precedente.

Cercare di ottenere gli attributi utente e le iscrizioni di gruppo se le credenziali sono accettate

Se questa opzione è selezionata, il test delle credenziali corretto tenta di verificare anche gli attributi utente e la ricerca del gruppo. Tenere presente che per il test corretto queste funzioni devono essere supportate e configurate nel fornitore di sicurezza.

Avvia test

Se il server è correttamente configurato e sono stati inseriti un nome utente e password di test validi, si riceverà un messaggio di conferma. In caso contrario, verrà visualizzato un messaggio di errore e un registro che consente di eseguire il debug del problema.

Fornitori di sicurezza :: Modifica - Kerberos

Impostazioni generali

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

Abilitato: Questo provider è abilitato

Se questa opzione è selezionata, il dispositivo Bomgar può cercare il fornitore di sicurezza quando un utente tenta l'accesso. Se l'opzione non è selezionata, il fornitore non sarà cercato.

Nomi utente e nomi visualizzati: Mantieni il nome del display sincronizzato con il sistema remoto

Questi valori stabiliscono i campi da utilizzare come nomi visualizzati privato e pubblico dell'utente.

Rimuovere REALM dai nomi principali

Selezionare questa opzione per rimuovere la parte del REALM dal principale nome utente nella costruzione del nome utente Bomgar.

Impostazioni di autorizzazione

Modalità di gestione utente

Selezionare gli utenti che possono autenticarsi sul dispositivo Bomgar. L'opzione **Consenti tutti gli utenti** consente chiunque si autentichi al momento mediante il KDC. L'opzione **Consentire soltanto dati principali dell'utente specificati nell'elenco** consente soltanto i dati principali dell'utente esplicitamente designati. L'opzione **Consentire soltanto dati principali dell'utente che corrispondono alla espressione regolare** consente soltanto i dati principali degli utenti che corrispondono all'espressione regolare compatibile Perl (PCRE).

Modalità di gestione SPN: Consenti soltanto gli SPN specificati nell'elenco

Se l'opzione non è selezionata, tutti i nomi principali del servizio (SPN) per questo fornitore di sicurezza sono consentiti. Se è selezionata, selezionare gli SPN specifici da un elenco di SPN configurati.

Ricerca del gruppo LDAP

Se si desidera che gli utenti su questo fornitore di sicurezza siano associati ai loro gruppi in un server LDAP separato, scegliere uno o più server di gruppo LDAP da utilizzare per la ricerca del gruppo.

Procedura di gruppo predefinito

Ogni utente autenticabile rispetto a un server esterno deve essere membro di almeno una procedura di gruppo per autenticarsi sul dispositivo Bomgar e deve accedere all'interfaccia /login o alla console di accesso. È possibile selezionare una procedura di gruppo predefinito da applicare a tutti gli utenti che sono autorizzati ad autenticarsi su un server configurato.

Procedure di sessione: Impostare le regole delle autorizzazioni di sessione e di prompt

Procedure di sessione

Le procedure di sessione consentono di personalizzare le autorizzazioni di sicurezza della sessione per ogni scenario specifico. Le procedure di sessione si possono applicare agli utenti e ai Jump Client.

Nella sezione **Procedure di sessione** vengono elencate le procedure disponibili. Fare clic sulla freccia con un nome della procedura per vedere rapidamente dove viene utilizzata la procedura, la disponibilità per gli utenti, gli inviti di accesso, i Jump Client e gli strumenti configurati.

Crea nuova procedura, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Copia

Per rendere più spedita la creazione di procedure di gruppo simili, cliccare su **Copia** per creare una nuova procedura con impostazioni identiche. Basta poi modificare questa nuova procedura in modo corrispondente ai requisiti specifici prescelti.

Procedura di sessione :: Aggiungi o Modifica

Impostazioni delle procedure

Nome display

Creare un nome univoco per consentire di identificare questo oggetto. Questo nome è di aiuto quando si assegna una procedura di sessione agli utenti e ai Jump Client.

Nome codice

Impostare un nome codice a scopi di integrazione. Se non si imposta un nome codice, ne verrà creato uno automaticamente.

Descrizione

Aggiungere una breve descrizione per riassumere lo scopo di questo oggetto. La descrizione viene visualizzata quando si applica una procedura agli account utente, alle procedure di gruppo e agli inviti di accesso.

Disponibilità: Utenti

Scegliere se tale procedura deve essere disponibile per l'assegnazione agli utenti (account utente e procedure di gruppo).

Disponibilità: Invito di accesso

Selezionare se deve essere disponibile per l'utilizzo da parte degli utenti quando invitano un utente esterno a partecipare a una sessione.

Disponibilità: Jump Clients

Scegliere se tale procedura deve essere disponibile per i Jump Client.

Disponibilità: Dipendenze

Se questa procedura di sessione è già in uso, verrà visualizzato il numero di utenti e di Jump Client che la utilizzano.

Strumenti

Per tutte le autorizzazioni che seguono, è possibile scegliere di attivare o disattivare l'autorizzazione oppure si può scegliere di impostarla su **Non definita**. Le procedure di sessione vengono applicate a una sessione in modo gerarchico con la massima priorità dei Jump Client, quindi agli utenti e alle impostazioni predefinite globali. Se a una sessione si applicano più procedure, la procedura con la priorità più alta avrà la precedenza sulle altre. Se, ad esempio, la procedura applicata a un Jump Client definisce un'autorizzazione, nessun'altra procedura può cambiare l'autorizzazione per la sessione. Per rendere un'autorizzazione disponibile per definire una procedura di livello inferiore, lasciare l'autorizzazione impostata su **Non definita**. Per i dettagli e gli esempi consultare Come utilizzare le procedure di sessione.

Impostare gli strumenti da abilitare o disabilitare con questa procedura.

Condivisione schermo

Consente all'utente di visualizzare o controllare lo schermo remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Limitazioni di condivisione applicazione

Limitare l'accesso a determinate applicazioni sul sistema remoto con l'opzione **Consenti soltanto gli eseguibili elencati** oppure **Rifiuta soltanto gli eseguibili elencati**. È anche possibile scegliere di consentire o rifiutare l'accesso al desktop.

> ***Nota:*** *questa funzione si applica soltanto ai sistemi operativi Windows e Linux e non comprende le sessioni Remote Desktop Protocol (RDP).*

Aggiungi nuovo(i) eseguibile(i)

Se vengono applicate le restrizioni sulla condivisione delle applicazioni, viene visualizzato un pulsante **Aggiungi nuovo(i) eseguibile(i)**. Facendo clic su questo pulsante si apre una finestra che consente di specificare i file eseguibili per negare o consentire, a seconda dei propri obiettivi.

Dopo aver aggiunto i file eseguibili, una o due tabelle mostrano i nomi dei file o gli hash selezionati per la restrizione. Un campo commenti modificabile consente note amministrative.

Inserire i nomi file o gli hash SHA-256, uno per riga

Quando si limitano gli eseguibili, inserire manualmente i nomi dei file eseguibili o gli hash che si desidera consentire o negare. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Cerca uno o più file

Quando si limitano gli eseguibili, selezionare questa opzione per navigare nel sistema e scegliere i file eseguibili per ricavare automaticamente i nomi o gli hash. Se si selezionano i file dalla piattaforma locale e dal sistema in questo modo, accertarsi che i file siano effettivamente file eseguibili. Non viene eseguita alcuna verifica a livello di browser.

Scegliere **Utilizzare il nome file** o **Utilizzare l'hash del file** in modo che il browser ricavi automaticamente i nomi o gli hash dei file eseguibili. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Nota: *questa opzione è disponibile solo nei browser moderni non in quelli precedenti.*

Limitazioni dell'endpoint consentite

Consente di impostare se l'utente può sospendere l'input del mouse e della tastiera del sistema remoto. L'utente può anche impedire al desktop remoto di essere visualizzato.

Consentito accedere utilizzando le credenziali di un gestore delle credenziali di endpoint

Abilitare la connessione di un utente al proprio Manager credenziali endpoint per utilizzare le credenziali dal proprio archivio password o insieme di credenziali esistenti.

L'utilizzo del Manager credenziali endpoint richiede un accordo separato sui servizi con Bomgar. Dopo aver stipulato l'accordo, è possibile scaricare il middleware richiesto dal centro self-service Bomgar.

Nota: *prima della versione 15.2, questa funzione era disponibile soltanto nelle sessioni avviate da Jump Client elevati su Windows®. A partire dalla versione 15.2, è possibile utilizzare un Manager credenziali endpoint nelle sessioni Jump remote, nelle sessioni Microsoft® Remote Desktop Protocol e nelle sessioni Shell Jump. è anche possibile utilizzare questa funzione con l'azione speciale Esegui come in una sessione di condivisione schermo su un sistema Windows®.*

Annotazioni

Consente all'utente di usare gli strumenti di annotazione per disegnare sullo schermo dell'utente remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Trasferimento file

Consente all'utente di caricare file nel sistema remoto, scaricare file dal sistema remoto o entrambe le operazioni. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Percorsi accessibili sul file system dell'endpoint

Consente all'utente di trasferire file a o da qualsiasi directory nel sistema remoto oppure solo a o da determinate directory.

Percorsi accessibili sul file system dell'utente

Consente all'utente di trasferire file a o da qualsiasi directory nel proprio sistema locale oppure solo a o da determinate directory.

Shell di comando

Consente all'utente di inserire comandi nel computer remoto tramite un'interfaccia virtuale della riga di comando. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Informazioni del sistema

Consente all'utente di vedere le informazioni di sistema sul computer remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Consentito utilizzare le azioni sulle informazioni di sistema

Consente all'utente di interagire con i processi e i programmi del sistema remoto senza richiedere la condivisione schermo. Arresto dei processi; avvio, arresto, pausa, ripresa e riavvio dei servizi e disinstallazione dei programmi.

Accesso al registro di sistema

Consente all'utente di interagire con il registro del sistema remoto Windows senza richiedere la condivisione schermo. Visualizzazione, aggiunta, eliminazione e modifica delle chiavi, ricerca e importazione/esportazione delle chiavi.

Script preconfezionati

Consente all'utente di eseguire script preconfezionati, creati per i suoi team. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Elevazione

Consente all'utente di tentare di elevare il client dell'endpoint per funzionare con diritti amministrativi nel sistema remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Salva procedura

Per rendere disponibile questa procedura, fare clic su **Salva procedura**.

Esporta procedura

È possibile esportare una procedura di sessione da un sito e importarne le autorizzazioni in una procedura su un altro sito. Modificare la procedura che si desidera esportare e scorrere verso il fondo della pagina. Fare clic su **Esporta procedura** e salvare il file.

Importa procedura

È possibile importare queste impostazioni in qualsiasi altro sito Bomgar che supporta l'importazione di procedure di sessione. Creare una nuova procedura di sessione e scorrere verso il fondo della pagina. Cercare il file della procedura e poi fare clic su **Importa procedura**. Caricato il file della procedura, la pagina viene aggiornata, consentendo di apportare modifiche. Per rendere disponibile la procedura, fare clic su **Salva procedura**.

Simulatore della procedura di sessione

Poiché l'organizzazione delle procedure può essere complessa, è possibile utilizzare il **Simulatore della procedura di sessione** per stabilire quale sarà il risultato. Inoltre, è possibile utilizzare il simulatore per risolvere il problema di un permesso non disponibile quando dovrebbe esserlo.

Utente

Iniziare selezionando l'utente che esegue la sessione. Questo menu a discesa include gli account utente e le procedure di invito di accesso.

Metodo di avvio sessione

Selezionare il metodo di avvio sessione. Può essere uno del **Jump Client**, **Jump remoto** o **Jump locale**.

Jump Client / Elemento Jump

Cercare un elemento Jump per nome, commenti, gruppo Jump o tag.

Simula

Fare clic su **Simula**. Nell'area sottostante, le autorizzazioni configurabili per procedura di sessione vengono visualizzate nella modalità di sola lettura. È possibile visualizzare le autorizzazioni consentite o negate a causa delle procedure in coda e la procedura impostata per ciascuna autorizzazione.

Procedure di gruppo: Applicare le autorizzazioni a gruppi di utenti

Procedure di gruppo

La pagina **Procedure di gruppo** consente di impostare gruppi di utenti con privilegi comuni.

Crea nuova procedura, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Copia

Per rendere più spedita la creazione di procedure di gruppo simili, cliccare su **Copia** per creare una nuova procedura con impostazioni identiche. Basta poi modificare questa nuova procedura in modo corrispondente ai requisiti specifici prescelti.

Modifica ordine

Fare clic su questo pulsante per trascinare le procedure di gruppo per l'impostazione della priorità. Per rendere effettive le modifiche dell'ordine di priorità, cliccare su **Salva ordine**. Per ragioni gestionali, l'ordine di priorità consigliato è di definire come più elevate (impedendone l'annullamento) le procedure di gruppo per gruppi di utenti specifici e meno elevate quelle per gruppi generici.

Procedura di gruppo :: Aggiungi o Modifica

Impostazioni di base

Codice di accesso e-mail

Abilita l'autenticazione a più fattori. Gli utenti ricevono una e-mail con un codice univoco di autenticazione ogni volta che accedono all'interfaccia amministrativa /login o alla console di accesso, desktop e mobile. Se per tre volte consecutive viene immesso il codice errato, è necessario immettere di nuovo le credenziali e ottenere un nuovo codice e-mail.

Nome della procedura

Creare un nome univoco per consentire di identificare questo oggetto.

Membri della procedura

Per assegnare membri fare clic sul pulsante **Aggiungi** per aprire una casella di selezione. Selezionare gli utenti dal sistema locale oppure selezionare gli utenti o interi gruppi dai fornitori di sicurezza configurati. Per aggiungere utenti o gruppi da una memoria di directory esterna come LDAP, RADIUS o Kerberos, è necessario configurare la connessione nella pagina **/login > Utenti e sicurezza > Fornitori di sicurezza**. Se il tentativo di aggiungere un utente da un provider di sicurezza configurato non è valido, viene visualizzato il messaggio di errore di registro di sincronizzazione qui e nel registro.

Impostazioni account

Definito in questa procedura

Selezionare per ogni impostazione se deve essere definita in questa procedura o lasciata disponibile ai singoli utenti per la configurazione. Se viene definita, non sarà possibile modificare il privilegio di un singolo utente nella pagina dell'account utente.

Se si ha una procedura che specifica un'autorizzazione e non si desidera che un'altra procedura possa sostituire tale autorizzazione, occorre selezionare che l'autorizzazione non possa essere annullata e la priorità di tale procedura deve essere più elevata di quella di altre procedure che definiscono ulteriormente l'impostazione in questione.

L'account scade il

Fa scadere l'account dopo una determinata data o non lo fa scadere mai.

Account disabilitato

Disattiva l'account in modo che l'utente non possa connettersi. La disattivazione NON cancella l'account.

Commenti

Inserire commenti per aiutare a identificare la finalità dell'oggetto.

Permessi

Amministratore

Concede all'utente pieni diritti amministrativi.

Consentito impostare password

Consente all'utente di impostare le password e di sbloccare gli account utente per gli utenti locali non amministrativi.

Consentito modificare i Jumpoint

Consente all'utente di creare o modificare i Jumpoints. Questa opzione non incide sulla capacità dell'utente di accedere a computer remoti tramite Jumpoint, che viene configurata per Jumpoint o procedura di gruppo.

Autorizzazioni report Sessione di accesso: Consentito visualizzare report delle sessioni di accesso

Consente a un utente di eseguire report sull'attività di sessione di accesso, visualizzando solo le sessioni di cui è il titolare principale, solo le sessioni in cui uno dei team era quello principale o uno dei suoi colleghi di team era il titolare di sessione principale oppure tutte le sessioni.

Consentito visualizzare registrazioni delle sessioni di accesso

Consente all'utente di vedere le registrazioni filmate di sessioni di condivisione schermo e della shell di comando.

Consentito usare report API

Consente di utilizzare le credenziali dell'utente da utilizzare per estrarre report XML tramite l'API.

Consentito usare il comando API

Consente di utilizzare le credenziali dell'utente per emettere comandi tramite l'API.

Consentito modificare team

Consente all'utente di creare o modificare i team.

Consentito modificare script preconfezionati

Consente all'utente di creare o modificare script preconfezionati da utilizzare nella condivisione schermo o in sessioni della shell di comando.

Consentito modificare i collegamenti personalizzati

Consente all'utente di creare o modificare i collegamenti personalizzati.

Autorizzazioni di accesso

Accesso

Consentito accedere agli endpoint

Consente all'utente di accedere alla console per eseguire sessioni. Se l'accesso all'endpoint è attivato, sono disponibili anche le opzioni di accesso all'endpoint.

Gestione sessione

Consentito condividere sessioni con i team a cui loro non appartengono

Consente all'utente di invitare un gruppo minore di utenti per condividere le sessioni, non solo i membri del proprio team. Se abbinata all'autorizzazione di disponibilità estesa, questa autorizzazione consente di espandere la propria capacità di condividere sessioni.

Consentito invitare utenti esterni

Consente all'utente di invitare un utente esterno a partecipare una tantum a una sessione.

Consentito abilitare la modalità Disponibilità estesa

Consente di ricevere e-mail di invito da altri utenti che chiedono di condividere una sessione quando non sono connessi alla console di accesso.

Consentito modificare la chiave esterna

Consente all'utente di modificare la chiave esterna nel pannello Informazioni sessione di una sessione nell'ambito della console di accesso.

Condivisione schermo da utente a utente

Consentito mostrare lo schermo ad altri utenti

Consente all'utente di condividere il proprio schermo con un altro utente senza che l'utente ricevente debba partecipare a una sessione. Questa opzione è disponibile anche se l'utente non è nella sessione.

Consentito dare il controllo quando si mostra lo schermo ad altri utenti

Consente all'utente di condividere il proprio schermo per dare il controllo di tastiera e mouse all'utente che visualizza lo schermo.

Tecnologia Jump

Metodi Jump consentiti: Consentito avviare sessioni da Jump Clients che utilizzano uno dei seguenti metodi Jump

Consente all'utente di eseguire il Jump a computer tramite **Jump Client**, **Jump locale sulla rete locale**, **Jump remoto mediante un Jumpoint**, **RDP mediante un Jumpoint** e/o **Shell Jump mediante un Jumpoint**.

Autorizzazioni elemento Jump: Consentito avviare sessioni da tutti gli elementi Jump del sistema

Consente all'utente di eseguire il Jump a computer remoti su tutti i gruppi Jump del team.

Autorizzato a distribuire, rimuovere e modificare elementi Jump nei seguenti gruppi Jump

Autorizza l'utente a vincolare sessioni, impostare gruppi e aggiungere commenti a elementi Jump solo per il gruppo Jump personale, per i team e i gruppi Jump dei membri del team oppure per tutti i gruppi Jump, compresi quelli distribuiti a team a cui l'utente non appartiene e a un qualsiasi Gruppo Jump personale di un utente.

Consentito modificare le procedure di sessione associate agli elementi Jump

Consente all'utente di impostare la procedura di sessione che deve utilizzare un elemento Jump. La modifica della procedura di sessione può influenzare le autorizzazioni consentite nella sessione.

Autorizzazioni sessione

Impostare le regole di prompt e di autorizzazione da applicare alle sessioni di questo utente. Scegliere una procedura di sessione esistente o definire le autorizzazioni personalizzate per questo utente. Se **non definita**, sarà utilizzata la procedura globale predefinita. Queste autorizzazioni possono essere sovrascritte da una procedura superiore.

Descrizione

Visualizza la descrizione di una procedura di autorizzazione di sessione predefinita.

Condivisione schermo

Condivisione schermo

Consente all'utente di visualizzare o controllare lo schermo remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Limitazioni di condivisione applicazione

Limitare l'accesso a determinate applicazioni sul sistema remoto con l'opzione **Consenti soltanto gli eseguibili elencati** oppure **Rifiuta soltanto gli eseguibili elencati**. È anche possibile scegliere di consentire o rifiutare l'accesso al desktop.

Nota: *questa funzione si applica soltanto ai sistemi operativi Windows e Linux e non comprende le sessioni Remote Desktop Protocol (RDP).*

Aggiungi nuovo(i) eseguibile(i)

Se vengono applicate le restrizioni sulla condivisione delle applicazioni, viene visualizzato un pulsante **Aggiungi nuovo(i) eseguibile(i)**. Facendo clic su questo pulsante si apre una finestra che consente di specificare i file eseguibili per negare o consentire, a seconda dei propri obiettivi.

Dopo aver aggiunto i file eseguibili, una o due tabelle mostrano i nomi dei file o gli hash selezionati per la restrizione. Un campo commenti modificabile consente note amministrative.

Inserire i nomi file o gli hash SHA-256, uno per riga

Quando si limitano gli eseguibili, inserire manualmente i nomi dei file eseguibili o gli hash che si desidera consentire o negare. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Cerca uno o più file

Quando si limitano gli eseguibili, selezionare questa opzione per navigare nel sistema e scegliere i file eseguibili per ricavare automaticamente i nomi o gli hash. Se si selezionano i file dalla piattaforma locale e dal sistema in questo modo, accertarsi che i file siano effettivamente file eseguibili. Non viene eseguita alcuna verifica a livello di browser.

Scegliere **Utilizzare il nome file** o **Utilizzare l'hash del file** in modo che il browser ricavi automaticamente i nomi o gli hash dei file eseguibili. Fare clic su **Aggiungi eseguibile(i)** al termine dell'aggiunta dei file scelti per la configurazione.

Si possono creare fino a 25 file per finestra di dialogo. Se è necessario aggiungerne altri, fare clic su **Aggiungi eseguibile(i)** e poi riaprire la finestra di dialogo.

Nota: *questa opzione è disponibile solo nei browser moderni non in quelli precedenti.*

Limitazioni dell'endpoint consentite

Consente di impostare se l'utente può sospendere l'input del mouse e della tastiera del sistema remoto. L'utente può anche impedire al desktop remoto di essere visualizzato.

Consentito accedere utilizzando le credenziali di un gestore delle credenziali di endpoint

Abilitare la connessione di un utente al proprio Manager credenziali endpoint per utilizzare le credenziali dal proprio archivio password o insieme di credenziali esistenti.

L'utilizzo del Manager credenziali endpoint richiede un accordo separato sui servizi con Bomgar. Dopo aver stipulato l'accordo, è possibile scaricare il middleware richiesto dal centro self-service Bomgar.

> ***Nota:*** *prima della versione 15.2, questa funzione era disponibile soltanto nelle sessioni avviate da Jump Client elevati su Windows®. A partire dalla versione 15.2, è possibile utilizzare un Manager credenziali endpoint nelle sessioni Jump remote, nelle sessioni Microsoft® Remote Desktop Protocol e nelle sessioni Shell Jump. è anche possibile utilizzare questa funzione con l'azione speciale Esegui come in una sessione di condivisione schermo su un sistema Windows®.*

Annotazioni

Consente all'utente di usare gli strumenti di annotazione per disegnare sullo schermo dell'utente remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Trasferimento file

Trasferimento file

Consente all'utente di caricare file nel sistema remoto, scaricare file dal sistema remoto o entrambe le operazioni. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Percorsi accessibili sul file system dell'endpoint

Consente all'utente di trasferire file a o da qualsiasi directory nel sistema remoto oppure solo a o da determinate directory.

Percorsi accessibili sul file system dell'utente

Consente all'utente di trasferire file a o da qualsiasi directory nel proprio sistema locale oppure solo a o da determinate directory.

Shell di comando

Shell di comando

Consente all'utente di inserire comandi nel computer remoto tramite un'interfaccia virtuale della riga di comando. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Informazioni del sistema

Informazioni del sistema

Consente all'utente di vedere le informazioni di sistema sul computer remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Consentito utilizzare le azioni sulle informazioni di sistema

Consente all'utente di interagire con i processi e i programmi del sistema remoto senza richiedere la condivisione schermo. Arresto dei processi; avvio, arresto, pausa, ripresa e riavvio dei servizi e disinstallazione dei programmi.

Accesso al registro di sistema

Accesso al registro di sistema

Consente all'utente di interagire con il registro del sistema remoto Windows senza richiedere la condivisione schermo. Visualizzazione, aggiunta, eliminazione e modifica delle chiavi, ricerca e importazione/esportazione delle chiavi.

Altri strumenti

Script preconfezionati

Consente all'utente di eseguire script preconfezionati, creati per i suoi team. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Elevazione

Consente all'utente di tentare di elevare il client dell'endpoint per funzionare con diritti amministrativi nel sistema remoto. Se **non definita**, questa opzione sarà impostata dalla successiva procedura di livello inferiore. Questa impostazione può essere sovrascritta da una procedura con priorità superiore.

Programma di login

Accesso dell'utente limitato al programma seguente

Impostare una programmazione per definire quando gli utenti possono accedere alla console. Impostare il fuso orario da utilizzare per la programmazione e aggiungere una o più voci di programmazione. Per ciascuna voce, immettere il giorno e l'ora di inizio e il giorno e l'ora di fine.

Se, ad esempio, è stato impostato l'inizio alle ore 8.00 e la fine alle ore 17.00, un utente può accedere in qualsiasi momento durante questa finestra temporale, ma può continuare a lavorare oltre il limite di fine impostato. Tuttavia non potrà riconnettersi dopo le 17.00.

Forza disconnessione quando il programma non consente il login

Se è richiesto il controllo degli accessi, selezionare questa opzione. In tal modo l'utente viene disconnesso all'ora di fine pianificata. In questo caso, l'utente inizia a ricevere notifiche ripetute 15 minuti prima della disconnessione. Quando un utente

viene disconnesso, tutte le sessioni pertinenti seguiranno le regole di fallback della sessione.

Iscrizioni

Team

Designa i team a cui devono essere aggiunti gli utenti di questo gruppo. Se un utente fa parte di un altro gruppo che aggiunge utenti a un team, ma l'utente non desidera che gli utenti di tale gruppo facciano parte di quel team, impostare la procedura in modo da rimuoverli da quel team. Gli utenti aggiunti manualmente a un team non possono essere rimossi mediante una procedura di gruppo.

Jumpoints

Designa i Jumpoints a cui gli utenti di questo gruppo hanno accesso.

Soltanto per le procedure di gruppo, se un utente fa parte di un altro gruppo che dà accesso a un Jumpoint, ma l'utente non desidera che gli utenti di tale gruppo abbiano accesso a quel Jumpoint, impostare la procedura in modo da rimuoverli da quel Jumpoint. Gli utenti aggiunti manualmente a un Jumpoint non possono essere rimossi mediante una procedura di gruppo.

Salva procedura

Per applicare la procedura, cliccare su **Salva procedura**.

Esporta procedura

È possibile esportare una procedura di gruppo da un sito e importarne le autorizzazioni in una procedura su un altro sito. Modificare la procedura che si desidera esportare e scorrere verso il fondo della pagina. Fare clic su **Esporta procedura** e salvare il file.

Nota: *quando si esporta una procedura di gruppo, vengono esportati solo nome, impostazioni di account e autorizzazioni di tale procedura. L'esportazione non include i membri della procedura, i membri del team e i membri di Jumpoint.*

Importa procedura

È possibile a questo punto importare le impostazioni della procedura di gruppo in qualsiasi altro sito Bomgar che supporta l'importazione di procedure di gruppo. Creare una nuova procedura di gruppo o modificarne una esistente di cui si desidera sostituire le autorizzazioni e scorrere verso il fondo della pagina. Cercare il file della procedura e poi fare clic su **Importa procedura**. Caricato il file della procedura, la pagina viene aggiornata, consentendo di apportare modifiche; per applicare la procedura, fare clic su **Salva procedura**.

Nota: *l'importazione di un file di procedura in una procedura di gruppo esistente sovrascrive le eventuali autorizzazioni definite in precedenza, ad eccezione di membri della procedura, membri del team e membri di Jumpoint.*

Scheda chiave Kerberos: Gestire la scheda chiave Kerberos

Gestione scheda chiave Kerberos

Bomgar supporta la funzionalità di accesso Single Sign-On con protocollo di autenticazione Kerberos. Questo consente agli utenti l'autenticazione per il dispositivo Bomgar senza dover inserire le credenziali. L'autenticazione Kerberos è valida per l'interfaccia Web /login e per la console di accesso.

Per integrare Kerberos con il dispositivo Bomgar, è indispensabile che Kerberos sia già installato o in corso d'installazione. Requisiti specifici:

- Occorre disporre di un Centro distribuzione chiavi (KDC) in funzione.
- Gli orologi devono essere sincronizzati per tutti i client, il KDC e il dispositivo Bomgar. Questa operazione può essere eseguita con la massima semplicità mediante un server Network Time Protocol (NTP).
- È indispensabile avere un Service Principal Name (SPN) creato nel KDC per il proprio dispositivo Bomgar.

Principali configurati

La sezione **Principali configurati** elenca tutti gli SPN disponibili per ogni keytab caricato.

Una volta che si dispone degli SPN, è possibile configurare un fornitore di sicurezza Kerberos nella pagina **Fornitori di sicurezza** e definire quali entità utente possono autenticare il dispositivo Bomgar tramite Kerberos.

Importa scheda chiave

Caricamento

Esportare il keytab per l'SPN dal KDC e caricarlo nel dispositivo Bomgar tramite la sezione **Importazione keytab** di questa pagina.

Report: Report sulle attività di sessione

Reports :: Accesso

Gli amministratori e gli utenti privilegiati possono creare ampi e dettagliati report e inoltre applicare filtri specifici per personalizzare le informazioni dei report secondo le loro specifiche necessità.

Tipo di report

Generare report di attività secondo tre distinti tipi di report: **Sessione**, **Sommario** e **Sessione Forensic** (se abilitato).

Filtri

Applicare opzioni di filtraggio, a seconda del caso, per ottenere ulteriori report personalizzati dai tipi di report basilari. Abilita uno o più filtri secondo la tua richiesta, ma verranno mostrate solo le sessioni che corrispondono a tutti i filtri selezionati.

ID sessione o numero di sequenza

Questo identificatore univoco richiede di specificare l'ID (LSID) o il numero di sequenza per la singola sessione ricercata. Ciò risulta utile se si dispone di un sistema esterno di ticket o a integrazione CRM. Non è possibile combinare questo filtro con altri.

Intervallo date

Selezionare una data di inizio per eseguire il pull dei dati di report. Selezionare quindi il numero dei giorni per i quali eseguire il pull del report o una data di fine.

Endpoint

Filtrare le sessioni in base al nome del computer, l'IP pubblico o l'IP privato.

Utente

Utilizzare il menu a discesa per selezionare il tipo di partecipazione dell'utente da includere. Scegliere le sessioni dove ha partecipato un determinato utente oppure ha partecipato un qualsiasi utente nell'ambito di un team comprese le sessioni che non sono mai state associate a quel team.

Chiave esterna

Filtro per sessioni di report che hanno utilizzato la stessa specifica chiave esterna.

Includi solo le sessioni completate

Filtrare per includere soltanto le sessioni completate. Sono escluse le sessioni ancora in corso.

Report Sessione di accesso

Visualizzare tutte le sessioni che corrispondono ai criteri specificati nella pagina precedente. I report di sessione comprendono le informazioni di base sulla sessione con i link ai dettagli della sessione, alle trascrizioni chat e alle registrazioni filmate di sessioni di condivisione schermo e della shell di comando.

Dettagli della sessione di accesso

I report di sessione indicano la registrazione della trascrizione completa delle chat, il numero dei file trasferiti e le azioni specifiche avvenute durante la sessione. Gli eventi Windows che presentano modifiche visive ovvie con una sessione vengono registrati come eventi nei dettagli della sessione. Ciò include essenzialmente le modifiche alla finestra in primo piano con il nome dell'eseguibile e il titolo della finestra.

Altri dati sulla sessione includono la durata della sessione, gli indirizzi IP locale e remoto e i dati del sistema remoto (se l'opzione è attivata). È possibile consultare i report online oppure scaricarli nel proprio sistema locale.

Se è stata attivata la funzione di registrazione sessione, è possibile vedere la riproduzione filmata di singole sessioni, compresa l'annotazione di chi controllava il mouse e la tastiera in qualsiasi momento durante la sessione. Se è stata attivata la funzione di registrazione prompt, è possibile vedere anche una registrazione e/o la trascrizione testo di tutte le shell di comando eseguite durante la sessione. Tutte le registrazioni sono archiviate nel dispositivo Bomgar in formato raw e convertite in formato compresso al momento della visualizzazione o del download.

Report di riepilogo degli accessi

I report del tipo Sommario offrono una panoramica sull'attività nel corso del tempo, suddivisa in categorie per utente. Le statistiche comprendono il numero totale delle sessioni eseguite, il numero medio di sessioni per giorno lavorativo e la durata media delle sessioni.

Reports :: Attività del team

Inizio intervallo, Durata, Fine intervallo

Selezionare una data di inizio per eseguire il pull dei dati di report. Selezionare quindi il numero dei giorni per i quali eseguire il pull del report o una data di fine.

Limita a

Scegliere il team di cui si desidera visualizzare i registri delle attività.

Report di attività del team

Visualizzare tutte le attività del team che corrispondono ai criteri specificati nella pagina precedente. I report di attività del team includono informazioni sugli utenti quando accedono o si disconnettono dalla console di accesso, i messaggi di chat inviati tra i membri del team, le azioni di condivisione dello schermo tra utenti e i file condivisi e scaricati.

Gestione

Gestione del software: Esegui un download di backup, aggiorna il software

Software :: Impostazioni di backup

Una delle migliori pratiche prevede il salvataggio regolare di una copia di riserva delle proprie impostazioni software da utilizzare per il recupero in caso di disastro. Bomgar consiglia di eseguire il backup della configurazione del proprio dispositivo Bomgar ogni volta che ne modifichi le impostazioni. In caso di guasto all'hardware, il file di backup rende più rapido il ripristino e, se necessario, consente a Bomgar di fornire all'utente l'accesso a servizi temporanei ospitati mantenendo le impostazioni del backup più recente.

Password di backup

Per proteggere con password il file di backup del so, creare una password. Se si sceglie la protezione con password, è impossibile recuperare la copia senza fornire la password.

Comprende il registro di accesso

Se questa opzione è selezionata, il file di backup includerà i registri di sessione. Deselezionando questa casella, si escluderanno i dati relazione della sessione dal backup.

Scarica backup

Salvare una copia della configurazione del software e metterla al sicuro. Salvare il file in una posizione sicura.

Software :: Ripristina impostazioni

File di backup

Se fosse necessario ricorrere al backup, sfogliare l'elenco dei file per selezionare il file di backup più recente tra quelli archiviati.

Password di backup

Se è stata creata una password per il file di backup, inserirla qui.

Carica backup

Caricare il file di backup nel dispositivo Bomgar e ripristinare le impostazioni del sito su quelle salvate nel backup.

Software :: Carica aggiornamento

Serviti della funzione **Carica aggiornamento software** per caricare manualmente i nuovi pacchetti software da Bomgar. Verrà chiesto di confermare che desideri caricare il pacchetto software. La sezione **Aggiornamento caricato** mostra informazioni aggiuntive utili a verificare il tuo pacchetto caricato. Fai clic su **Installa** se desideri completare il processo di installazione, o su **Elimina aggiornamento** se desideri annullare la sezione di preparazione all'aggiornamento. Se il pacchetto di aggiornamento contiene unicamente licenze aggiuntive, è possibile installare l'aggiornamento senza riavviare il dispositivo. Dopo aver confermato che desideri installare, la pagina visualizzerà una barra di progresso per consentirti di seguire l'avanzamento complessivo dell'installazione. Gli aggiornamenti qui eseguiti aggiornano automaticamente tutti i siti e le licenze del dispositivo Bomgar.

Nota: *l'amministratore del dispositivo Bomgar può anche usare la funzione* ***Controlla aggiornamenti*** *dell'interfaccia del dispositivo per cercare e installare automaticamente nuovi pacchetti software.*

Sicurezza: Gestire le impostazioni di sicurezza

Sicurezza :: Opzioni

Lunghezza minima della password

Impostare le regole per gli account degli utenti locali sulla lunghezza delle password.

Richiedi password complesse

È possibile impostare regole per gli account degli utenti locali circa la complessità delle password.

Scadenza predefinita password

È possibile impostare regole per gli account degli utenti locali circa la frequenza di scadenza delle password.

Abilita reimpostazione password

È possibile impostare regole per gli account degli utenti locali circa la possibilità di ripristinare una password dimenticata dopo aver fornito la risposta esatta a una domanda di sicurezza.

Abilita login salvati

Consentire o meno che la console di accesso ricordi le credenziali di un utente.

Esclusione dell'Account dopo

Impostare il numero di volte che una password errata può essere immessa prima che l'account sia bloccato.

Termina la sessione se l'account è in uso

Se un utente cerca di connettersi alla console di accesso con un account già in uso, la casella di controllo selezionata **Termina sessione** disconnette la connessione precedente per consentire la nuova connessione.

Modalità di sincronizzazione appunti

Modalità di sincronizzazione appunti determina come gli utenti sono autorizzati a sincronizzare gli Appunti nell'ambito di una sessione di condivisione schermo. Le impostazioni disponibili sono le seguenti:

- **Non autorizzato** - L'utente non può accedere né modificare gli Appunti del computer remoto.
- - L'utente può fare clic su un pulsante per copiare il contenuto degli Appunti locali negli Appunti del computer remoto.
- **Autorizzato all'invio manuale di Appunti in una direzione o nell'altra** - L'utente può fare clic su un pulsante per copiare il contenuto degli Appunti locali negli Appunti del computer remoto oppure può copiare il contenuto degli Appunti remoti nei propri Appunti locali.
- **Invia automaticamente modifiche degli Appunti in entrambe le direzioni** – Il contenuto di entrambi gli Appunti, locale e remoto, resta automaticamente lo stesso.

Perché questa impostazione diventi effettiva, si DEVE riavviare il software nella pagina di stato.

Convalida del certificato SSL

Se non è possibile convalidare adeguatamente la catena di certificazione, la connessione non viene autorizzata.

Se la convalida del certificato era stata prima disattivata e poi attivata, l'aggiornamento a questa impostazione è automatico per tutte le console del tecnico di supporto e i client al momento della connessione successiva. Tenere presente che l'upgrade degli agenti di connessione LDAP non è automatico, quindi si rende necessario reinstallarli per rendere effettiva l'impostazione.

Se viene attivata la **Convalida del certificato SSL**, oltre alle misure integrate di protezione Bomgar vengono eseguiti controlli di sicurezza per convalidare la catena di certificazione SSL adottata a protezione della comunicazione. La convalida SSL è un'impostazione vivamente consigliata. Se la convalida del certificato è disattivata, sull'interfaccia amministrativa viene visualizzato un messaggio di avvertenza. È possibile nascondere questo messaggio per trenta giorni.

> ***Nota:*** *per abilitare la convalida del certificato SSL, fornire a Bomgar la certificazione SSL in modo che questa venga incorporata all'interno del proprio software Bomgar.*

Giorni per conservare i dati di logging

In **Giorni di conservazione i dati di accesso**, è possibile impostare per quanto tempo i dati di accesso debbano essere archiviati sul dispositivo. Tali informazioni includono i dati di report e le registrazioni della sessione.

Chiave precondivisa di comunicazione tra dispositivi

Inserire una password nel campo **Chiave di comunicazione precondivisa interdispositivo** per stabilire una relazione approvata tra due dispositivi. Sono necessarie chiavi corrispondenti per configurare due o più dispositivi con funzioni quali failover o gruppo. La chiave deve contenere almeno 6 caratteri e una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale.

Sicurezza :: Limitazioni di rete

È possibile anche determinare quali reti IP devono essere in grado di accedere al proprio dispositivo Bomgar /login e /api.

Consenti da qualsiasi rete

Non viene applicata alcuna limitazione di rete.

Consenti soltanto le seguenti reti

Soltanto gli indirizzi IP elencati possono accedere al dispositivo Bomgar su /login o /api.

Rifiuta soltanto le seguenti reti

Tutti gli indirizzi IP eccetto quelli elencati possono accedere al dispositivo Bomgar su /login o /api.

Se si seleziona **Solo alla prima autenticazione dell'utente**, l'utente deve trovarsi su una rete consentita la prima volta che accede alla console di accesso. In quel momento, viene emesso un token per il dispositivo in modo che sia possibile accedere successivamente alla console di accesso da una qualsiasi postazione di rete.

Se si seleziona **Sempre**, l'utente deve trovarsi su una rete consentita ogni volta che accede alla console di accesso.

Se si seleziona **Mai**, l'utente può accedere alla console di accesso da qualsiasi postazione di rete.

Sicurezza :: Limitazioni di porte per interfaccia Web di gestione

Consente di impostare le porte utilizzate per l'accesso dall'interfaccia /login.

Configurazione del sito: Importare le porte HTTP /Abilita Prerequisito Accordo sui login

Sito :: HTTP

Porta HTTP e porte HTTPS

Esperti tecnici di rete che operano in ambienti non standard di rete possono cambiare le porte del traffico Bomgar. Le impostazioni di tali porte devono essere regolate solo nel caso in cui per l'accesso Internet si utilizzino porte diverse da quelle standard (80 e 443).

Sito :: /login Prerequisito Accordo sui login

Abilita accordo sui login

È possibile attivare un accordo di accesso che gli utenti devono accettare prima di accedere all'interfaccia amministrativa di /login. L'accordo configurabile consente di specificare le limitazioni e le regole delle procedura interne prima che gli utenti siano autorizzati a eseguire il login.

Titolo dell'accordo

Personalizzare titolo dell'accordo.

Testo dell'accordo

Fornire il testo per il contratto di accesso.

Configurazione e-mail: Configurazione del software per l'invio di e-mail

Configurazione :: Indirizzo email

Nota: *se un dispositivo è progettato come dispositivo di backup o di un nodo di traffico, la configurazione e-mail per tale dispositivo verrà sovrascritta con la configurazione e-mail definita nel dispositivo master primario.*

Da indirizzo

Impostare l'indirizzo e-mail dal quale verranno inviati i messaggi automatici del dispositivo Bomgar.

Configurazione :: Server di inoltro SMTP

È possibile configurare il dispositivo Bomgar in modo che funzioni assieme al relay server SMTP per l'invio automatico di avvisi e-mail su determinati eventi.

Server di inoltro SMTP

Immettere il nome host o l'indirizzo IP del server di inoltro SMTP.

Porta SMTP

Impostare la porta SMTP per contattare questo server.

Cifratura SMTP

Se il proprio server SMTP supporta la cifratura SSL, selezionare **SSL** o **TLS**. In caso contrario, selezionare **Nessuno**.

Nome utente SMTP

Se il proprio server SMTP richiede un'autenticazione, inserire un nome utente.

Password SMTP

Se il proprio server SMTP richiede un'autenticazione, inserire una password.

Configurazione :: Contatto di ammin.

Indirizzi e-mail del contatto di ammin. predefinito

Inserire uno o più indirizzi e-mail ai quali essere inviati le e-mail. Separare gli indirizzi con uno spazio.

Invia una email di prova una volta salvate le impostazioni

Se si desidera ricevere un'immediata e-mail di prova per verificare che le impostazioni SMTP siano configurate correttamente, selezionare questa opzione prima di fare clic sul pulsante **Salva modifiche**.

Invia avviso di comunicazione giornaliero

Si può impostare il dispositivo Bomgar a inviare un avviso giornaliero per confermare che la comunicazione di avvisi funziona correttamente.

Oltre all'e-mail di prova e alle note di comunicazione giornaliere che si possono configurare sopra, le e-mail vengono inviate per gli eventi seguenti:

- Durante operazioni di failover, la versione del prodotto sul nodo principale non corrisponde alla versione del prodotto sul nodo di backup.
- Durante il controllo dello stato di failover, viene rilevato uno dei problemi seguenti.
    - Il dispositivo corrente è il nodo principale e in /login è configurato un indirizzo IP condiviso ma l'interfaccia di rete non è abilitata.
    - In /login è configurato un indirizzo IP ma non è elencato come indirizzo IP in /appliance.
    - Il nodo di backup non è riuscito a contattare il nodo principale e neanche uno degli indirizzi IP di test configurati nella pagina **Gestione > Failover**.
    - Il nodo di backup non è riuscito a contattare nessuno degli indirizzi IP di test configurati nella pagina **Gestione > Failover**.
    - Le operazioni di backup del nodo sono disabilitate nella pagina **Gestione > Failover**.
    - Il nodo di backup inaspettatamente non è riuscito a eseguire una prova di se stesso, il che indica che è malfunzionante.
    - Il nodo di backup non è riuscito a contattare il nodo principale utilizzando il nome host del nodo principale.
    - Il failover automatico è disattivato e il nodo di backup non è riuscito a testare il nodo principale.
    - Il failover automatico è attivato e il nodo di backup non è riuscito a testare il nodo principale. Il nodo di backup diventerà automaticamente il nodo principale se il nodo principale rimane insensibile.
    - Il failover automatico è attivato e il nodo di backup sta diventando automaticamente il nodo principale poiché il nodo principale è rimasto inattivo troppo a lungo.
    - Il nodo principale a volte non è riuscito a eseguire una sincronizzazione dei dati con il nodo di backup nelle ultime 24 ore.

Eventi in uscita: Impostare gli eventi che avviano i messaggi

Eventi in uscita :: Destinatari HTTP

È possibile configurare il dispositivo Bomgar per inviare messaggi a un server HTTP oppure a un indirizzo e-mail quando vengono attivati eventi diversi.

Le variabili inviate dal dispositivo Bomgar arrivano come metodo POST HTTP e sono accessibili mediante la chiamata del metodo usato per il recupero dei dati POST nel linguaggio di codifica dell'utente. Se il server non risponde con un HTTP 200 per indicare che l'operazione è riuscita, il dispositivo Bomgar rimette in coda l'evento corrente e riprova in un momento successivo.

Aggiungi nuovo destinatario HTTP, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Eventi in uscita :: Aggiungi o Modifica destinatario HTTP

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

URL

Immettere un URL di destinazione per questo gestore eventi in uscita.

Disabilitato

Utilizzare la casella di controllo **Disabilitato** per interrompere rapidamente i messaggi del meccanismo di gestione eventi impostato come, ad esempio, nell'evento di test di integrazione pianificato.

Certificato CA

Se si opera su connessione HTTPS, è possibile caricare il certificato root CA indicato da un server eventi in uscita.

Eventi da inviare

Selezionare gli eventi che avviano i messaggi da inviare.

Intervallo riprova

Impostare la frequenza dei tentativi da eseguire in caso di insuccesso.

Durata riprova

Se un evento continua a provare ma non riesce, impostare per quanto tempo possa continuare a provare prima che venga abbandonato.

Contatto email

Inserire uno o più indirizzi e-mail ai quali deve essere inviato un avviso in caso di errore.

Invia avviso email dopo

Impostare quanto tempo dopo un errore l'e-mail deve essere inviata; se il problema viene risolto prima di questa scadenza e l'evento ha successo, l'avviso di errore non verrà inviato.

Invia di nuovo avvisi email

Impostare la frequenza di invio di e-mail se permane lo stato di errore.

Eventi in uscita :: Destinatari e-mail

Aggiungi nuovo destinatario e-mail, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

Stato attuale

Visualizza un breve messaggio di stato del server di inoltro SMTP. Fino a quando il dispositivo è in grado di inviare messaggi al server di inoltro, lo stato sarà **OK**. In caso contrario, rivedere le impostazioni del server di inoltro SMTP.

Durata riprova

Se un evento continua a provare ma non riesce, impostare per quanto tempo possa continuare a provare prima che venga abbandonato.

Eventi in uscita :: Aggiungi destinatario e-mail

Prima di impostare il dispositivo Bomgar per inviare messaggi di evento a un indirizzo e-mail, verificare che il dispositivo Bomgar sia configurato per funzionare con il server di inoltro SMTP. Passare alla pagina **Gestione > Configurazione e-mail** per verificare le impostazioni.

Nome

Creare un nome univoco per consentire di identificare questo oggetto.

Indirizzo email

Immettere l'indirizzo e-mail per ricevere la notifica degli eventi selezionati. Si possono configurare fino a dieci indirizzi e-mail separati da virgola.

Disabilitato

Utilizzare la casella di controllo **Disabilitato** per interrompere rapidamente i messaggi del meccanismo di gestione eventi impostato come, ad esempio, nell'evento di test di integrazione pianificato.

Richiedi chiave esterna

Se questa opzione è selezionata, le e-mail saranno inviate soltanto per le sessioni che hanno una chiave esterna nel momento in cui si verifica l'evento.

Eventi da inviare

Selezionare gli eventi che avviano i messaggi da inviare.

Oggetto

Personalizzare l'oggetto di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Testo

Personalizzare il corpo di questa e-mail. Utilizzare una delle macro elencate sotto questo capo nella pagina /login per personalizzare il testo secondo le proprie esigenze.

Failover: Impostare un dispositivo di backup per il failover

Failover :: Configurazione

Dettagli di connessione del nuovo sito di backup: Nome host o indirizzo IP

Immettere il nome host o l'indirizzo IP del dispositivo Bomgar da utilizzare per il backup in un rapporto di failover.

Porta TLS

Immettere la porta TLS che consente a questo dispositivo primario di connettersi al dispositivo di backup.

Inverti i dettagli di connessione a questo sito principale: Nome host o indirizzo IP

Immettere il nome host o l'indirizzo IP del dispositivo Bomgar da utilizzare come primario in un rapporto di failover.

Porta TLS

Immettere la porta TLS che consente al dispositivo di backup di connettersi al dispositivo primario.

Failover :: Stato

Stato di questo host

Visualizzare il nome host di questo sito e lo stato dell'istanza del sito primario o del sito di backup.

Stato dell'host peer

Visualizzare il nome host di questo sito e lo stato dell'istanza del sito primario o del sito di backup. Visualizzare inoltre la data e l'ora dell'ultimo controllo di stato.

Cronologia stato

Espandere o comprimere una tabella contenente gli eventi di stato verificatisi.

Failover :: Stato dell'istanza del sito primario o di backup

Il testo conferma se ci si trova sul sito primario o di backup del sito host.

Sincr ora

Forzare manualmente una sincronizzazione dati dal dispositivo primario nel dispositivo di backup.

Diventa backup/principale

Scambia i ruoli con il dispositivo peer forzando un failover per la manutenzione pianificata o un evento di failover conosciuto.

Contrassegnare questa casella per eseguire una sincr-dati dal sito all'indirizzo example.com mentre diventa il sito di backup/principale.

Selezionare la casella di controllo per sincronizzare i dati da un dispositivo peer prima di scambiare i ruoli. Se la casella di controllo è selezionata, tutti gli utenti sul dispositivo primario esistente saranno disconnessi durante la sincronizzazione dati e qualsiasi altra operazione non sarà disponibile fino al completamento dello scambio.

Selezionare questa casella per diventare un backup anche se è impossibile contattare il sito peer all'indirizzo example.com.

Nell'istanza del sito primario, si può scegliere di diventare backup anche se non è possibile contattare il dispositivo peer. Se questa opzione non è selezionata, il failover sarà annullato se entrambi i dispositivi non possono essere sincronizzati secondo i ruoli di failover (uno primario e uno backup).

Ad esempio, se si sa che il dispositivo di backup corrente è online, ma non può essere raggiunto dal primario a causa di un problema di connessione di rete, si potrebbe selezionare questa opzione per rendere backup il primario prima che venga ripristinata la connessione di rete. In questo esempio, potrebbe essere necessario accedere al backup corrente per renderlo primario.

Interrompi rapporti di failover

Consente di interrompere la relazione di failover rimuovendo tutti i dispositivi dal ruolo primario o di backup.

Failover :: Configurazione dell'istanza del sito primario o di backup

IP condivisi

Consente di controllare l'indirizzo IP condiviso utilizzato dal sito in caso di un evento di failover, selezionando la casella di controllo per l'indirizzo IP di failover. Se si modifica il rapporto tra siti, gli indirizzi IP visualizzati vengono disattivati quando un sito primario diventa di backup e attivati quando quello di backup diventa primario. Si consiglia di copiare manualmente l'impostazione sul sito peer giacché questa non viene condivisa.

Failover :: Impostazioni di backup

Le impostazioni qui configurate vengono abilitate solamente quando il sito configurato è nel ruolo di backup.

Nel sito principale, selezionare **Impostazioni di backup >** per espandere o ridurre la pagina in cui sono visualizzati i campi di configurazione.

Abilita operazioni di backup

Abilitare o disabilitare i backup del sito.

Intervallo di sincronizzazione dati non valido

È possibile controllare i dettagli dell'Intervallo di sincronizzazione dati automatico.

Limite di larghezza di banda sincr-dati

Imposta i parametri della larghezza di banda per la sincronizzazione dei dati.

Abilita Failover automatico

Consente di abilitare o disabilitare velocemente il failover automatico.

Timeout del sito principale

Consente di impostare i parametri temporali in base ai quali il sito primario non risulterà raggiungibile prima del failover.

IP di collaudo della connettività di rete

Immettere gli indirizzi IP per il sito di backup in modo da controllare se il backup non è in grado di raggiungere il sito primario perché quest'ultimo è offline o perché il backup ha perso la connessione di rete.

Configurazione API: Abilitare l'API XML e configurare i campi personalizzati

API :: Configurazione

Abilita XML API

Scegliere di abilitare l'API XML Bomgar, che consente di eseguire comandi per report e problemi, come l'avvio o il trasferimento di sessioni da applicazioni esterne nonché il backup automatico della configurazione del software.

Nota: *con questa impostazione vengono abilitati/disabilitati soltanto* ***Comando***, ***Reporting*** *e le chiamate* ***API dello script del client****. Le altre chiamate API sono configurate nei portali pubblici. Per istruzioni dettagliate, consultare la Guida di programmazione dell'API.*

Consenti accesso HTTP a XML API

Per impostazione predefinita, l'accesso all'API è protetto da codifica SSL. Tuttavia si può scegliere di consentire l'accesso HTTP, che è privo di codifica. Una delle migliori pratiche di protezione vivamente consigliabile è di non consentire l'accesso HTTP.

API :: Campi personalizzati

Creare campi API personalizzati per raccogliere informazioni sul cliente, che consentono di integrare più profondamente Bomgar nei propri programmi. I campi personalizzati devono essere utilizzati con l'API Bomgar. Per istruzioni dettagliate, consultare la Guida di programmazione dell'API.

Crea nuovo campo, Modifica, Elimina

Creare un nuovo oggetto, modificare un oggetto esistente oppure rimuovere un oggetto esistente.

API :: Campi personalizzati :: Aggiungi o Modifica

Nome display

Creare un nome univoco per consentire di identificare questo oggetto. Questo nome viene visualizzato nella console di accesso nei dettagli di sessione.

Nome codice

Impostare un nome codice a scopi di integrazione. Se non si imposta un nome codice, ne verrà creato uno automaticamente.

Mostra nella console di accesso

Se si seleziona **Mostra nella console di accesso**, questo campo e i rispettivi valori saranno visibili dove vengono visualizzati i dettagli della sessione personalizzata nella console di accesso.

Supporto tecnico: Rivolgersi al supporto tecnico Bomgar

Informazioni per contattare il supporto tecnico Bomgar

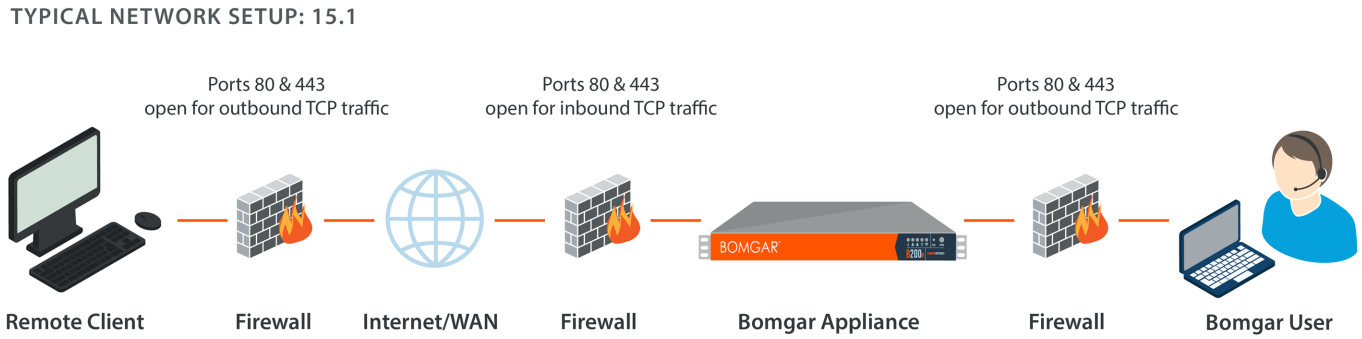
La pagina di supporto tecnico offre i dati di contatto nel caso ci si debba rivolgere a un tecnico di supporto clienti Bomgar.

Supporto tecnico avanzato fornito da Bomgar

Il tecnico di supporto clienti Bomgar che deve accedere al dispositivo del cliente, gli fornisce i codici di supporto, accesso e bypass da inserire in questa pagina per creare un canale di supporto diretto con Bomgar, pienamente codificato e attivato dal dispositivo per la risoluzione rapida di problemi complessi.

Porte e firewall

Le soluzioni Bomgar sono progettate per funzionare in modo trasparente attraverso firewall, consentendo la connessione con qualsiasi computer dotato di connettività Internet in qualsiasi parte del mondo. Tuttavia è possibile che sia necessario eseguire qualche configurazione per alcune reti a protezione elevata.



- Per il traffico TCP in uscita nel firewall del sistema remoto e dell'utente locale, devono essere aperte le porte 80 e 443. A seconda della propria build potrebbero essere disponibili più porte. Lo schema illustra una tipica configurazione di rete; per maggiori informazioni, consultare la Guida all'installazione dell'hardware del dispositivo Bomgar.
- Il software di protezione Internet, come i firewall, non deve impedire la possibilità di scaricare file eseguibili Bomgar. Alcuni esempi di firewall sono McAfee Security, Norton Security e Zone Alarm. Chi ha un firewall potrebbe incorrere in qualche problema di connessione. Per evitare questi problemi, configurare il proprio firewall a consentire di scaricare i seguenti file eseguibili, in cui {uid} è un identificatore esclusivo composto di lettere e numeri:
  - bomgar-pec-{uid}.exe
  - bomgar-pec.exe

  Per supporto nella configurazione del firewall, contattare il produttore del firewall.
- Per le regole del firewall di esempio basate sulla posizione del dispositivo, consultare www.bomgar.com/docs/content/deployment/dmz/firewall-rules.htm.

Nel caso si continui ad avere qualche difficoltà a stabilire la connessione, rivolgersi al supporto tecnico Bomgar all'indirizzo help.bomgar.com.

Declino di responsabilità, restrizioni di licenza e supporto tecnico

Dichiarazioni di responsabilità

Questo documento è fornito a scopo puramente informativo. Bomgar Corporation può variare i contenuti del presente documento senza notifica. Non si garantisce che il presente documento sia privo di errori o soggetto ad altre garanzie o condizioni espresse oralmente o implicite per legge, incluse garanzie implicite e condizioni di commerciabilità o idoneità a uno specifico scopo. Bomgar Corporation è esonerata da ogni responsabilità rispetto ai contenuti di questo documento tramite il quale non si forma, direttamente o indirettamente, alcuna obbligazione contrattuale. Le tecnologie, le funzionalità, i servizi e i processi descritti nel presente documento sono soggetti a modifiche senza preavviso.

BOMGAR, BOMGAR BOX, mark B, JUMP e UNIFIED REMOTE SUPPORT sono marchi registrati di Bomgar Corporation; gli altri marchi mostrati sono proprietà dei rispettivi titolari.

Limitazioni di licenza

La licenza Privileged Access Management di Bomgar consente l'accesso a un solo sistema dell'endpoint. Anche se questa licenza può essere trasferita da un sistema ad un altro se non è più necessario l'accesso per il primo sistema, sono necessarie due o più licenze (una per endpoint) per consentire l'accesso a più endpoint contemporaneamente.

Supporto tecnico

Bomgar è impegnata a offrire un'assistenza di altissimo livello, garantendo che i suoi clienti abbiano tutto il necessario per operare con la massima produttività. Per qualsiasi tipo di supporto, rivolgersi al supporto tecnico Bomgar all'indirizzo help.bomgar.com.

Il supporto tecnico viene offerto con l'acquisto annuale di un piano di manutenzione.