BOMGAR™

Privileged Access Management
Privileged Web

TC:9/28/2016

Indice

Indice 2
Guida Console di accesso Privileged Web 3
Requisiti della Console di accesso Privileged Web 4
Avviare la Console di accesso Privileged Web mediante /login 5
Utilizzare gli elementi Jump per accedere agli endpoint nella Console di accesso Privileged Web 7
Accedere agli endpoint utilizzando l'inserimento delle credenziali 10
Requisiti di sistema 10
Autenticazione dall'URL dell'API dello script del client 15
Tornare a una sessione attiva nella Console di accesso Privileged Web 16
Controllo dell'endpoint remoto con la condivisione dello schermo 17
Accedere alla shell di comando sull'endpoint remoto 19
Condivisione di una sessione con altri utenti che utilizzano la Console di accesso Privileged Web 20
Invitare un utente esterno a partecipare a una sessione 22
Rimuovere un membro da una sessione della Console di accesso Privileged Web 23
Chiudi sessione della Console di accesso Privileged Web 24
Scaricare il desktop nativo dalla Console di accesso Privileged Web 25

Guida Console di accesso Privileged Web

Grazie alla Console di accesso Privileged Web Bomgar, i team Informazioni e sicurezza cyber possono concedere agli utenti con privilegi l'accesso remoto sicuro ai sistemi critici, anche quando gli utenti non hanno la possibilità di installare il software nei propri ambienti desktop. Possono invece accedere agli endpoint mediante la console di accesso basata su Web. Ciò consente di concedere sempre l'accesso necessario e consente ai proprietari di sistema di soddisfare le esigenze aziendali quali il tempo di attività del sistema e le altre regole interne o esterne senza compromettere le difese messe in atto per proteggere l'organizzazione da ogni tipo di minaccia informatica dannosa.

In questa guida viene spiegato in particolare la Console di accesso Privileged Web e come questa console di accesso, basata su browser, accede agli endpoint ed esegue altre funzioni necessarie, garantendo nel contempo che venga mantenuto il più alto livello di sicurezza.

Nota: *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. Per qualsiasi tipo di supporto, rivolgersi al supporto tecnico Bomgar all'indirizzo help.bomgar.com.*

Requisiti della Console di accesso Privileged Web

Per eseguire la Console di accesso Privileged Web sul sistema, il dispositivo Bomgar deve eseguire la versione software 15.3 o superiore. Console di accesso Privileged Web è supportata sulle piattaforme e sui browser seguenti:

Piattaforme

- Windows
- Macintosh
- Linux

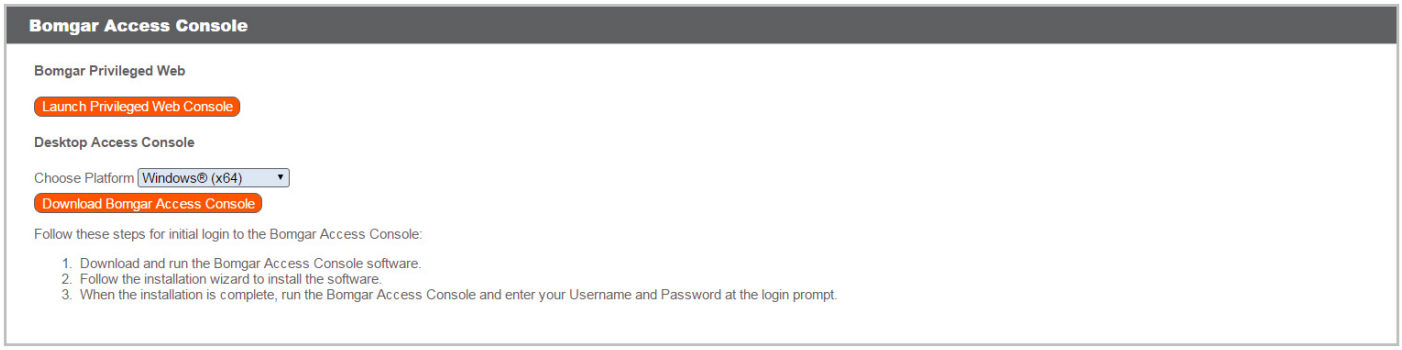
Browser

- Firefox 42+
- Chrome 46+
- Safari 8+
- Windows Edge

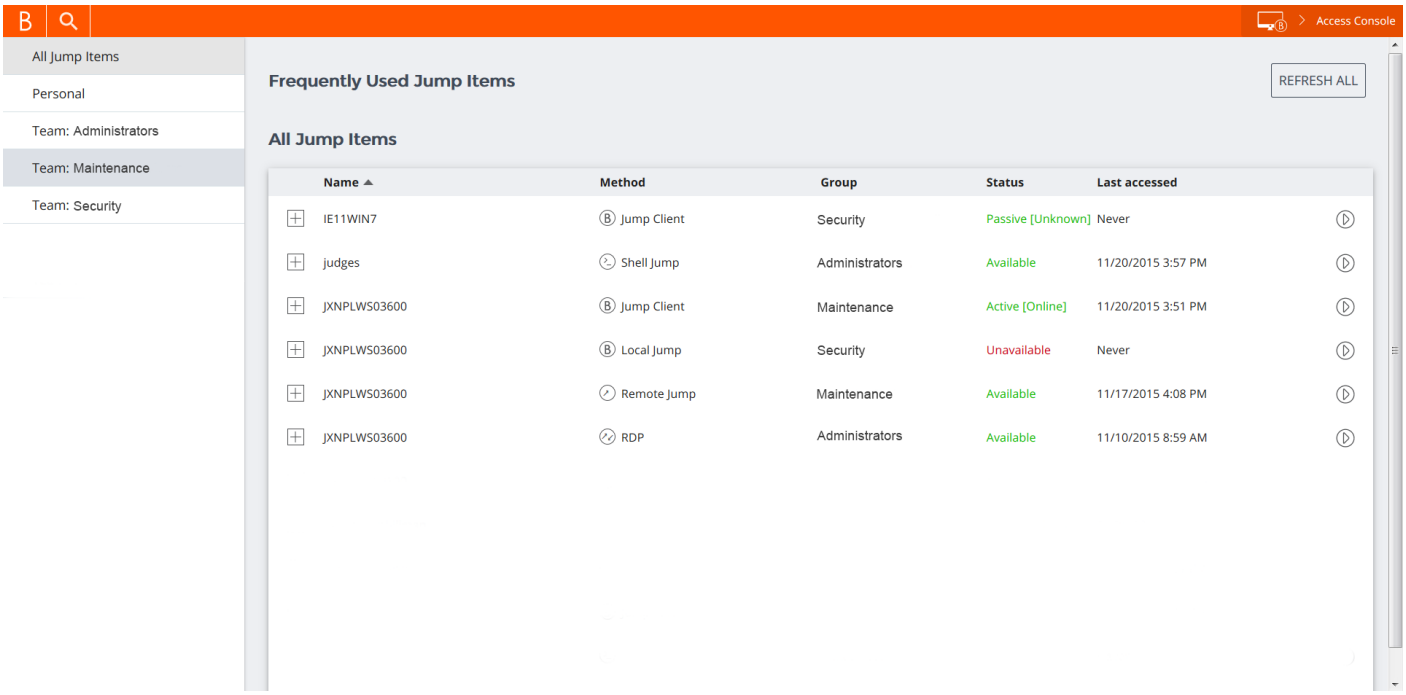
Avviare la Console di accesso Privileged Web mediante /login

La Console di accesso Privileged Web consente all'utente di utilizzare la console di accesso basata su Web per l'accesso protetto agli endpoint connettendoli da remoto tramite il dispositivo Bomgar. Per iniziare a utilizzare la Console di accesso Privileged Web per accedere agli endpoint seguire i passaggi descritti di seguito:

Nota: *Per impostazione predefinita, il* ***pulsante Avvia Privileged Web*** *non è disponibile. È necessario passare a Gestione <Sicurezza e selezionare "Abilita Privileged Web" per attivare la console.*

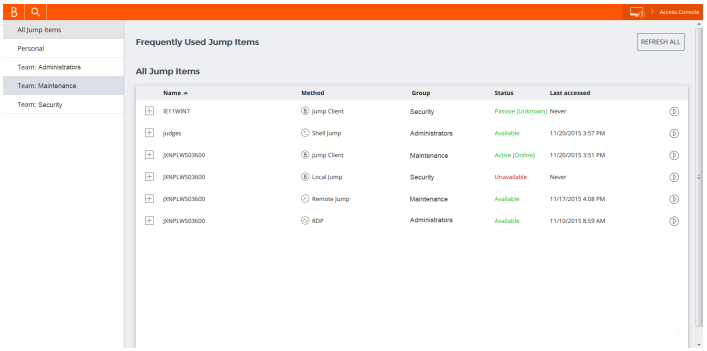


1. Nella barra degli indirizzi del browser, immettere il nome host del sito Bomgar, ad esempio access.example.com.
2. Immettere il nome utente e la password associati all'account utente Bomgar. È possibile scegliere che la console di accesso Bomgar ricordi le credenziali di accesso.
3. Fare clic su **Login**.
4. Dopo aver eseguito l'accesso all'interfaccia amministrativa /login, fare clic sulla scheda **Il mio account**.
5. Successivamente fare clic sul pulsante **Avvia Console di accesso Privileged Web** presente nella sezione **Console di accesso Bomgar**.
6. Si apre la Console di accesso Privileged Web nella nuova scheda ed è possibile iniziare ad accedere agli endpoint.



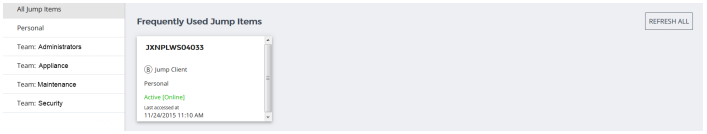
Utilizzare gli elementi Jump per accedere agli endpoint nella Console di accesso Privileged Web

Per accedere a un endpoint, installare un elemento Jump in quel sistema dalla pagina **Jump Client** dell'interfaccia amministrativa /login.



> ***Nota:*** *le autorizzazioni di account del tecnico di supporto potrebbero non consentirgli di usare Jump Client oppure consentirgli di eseguire un Jump, ma non di distribuire personalmente i client.*

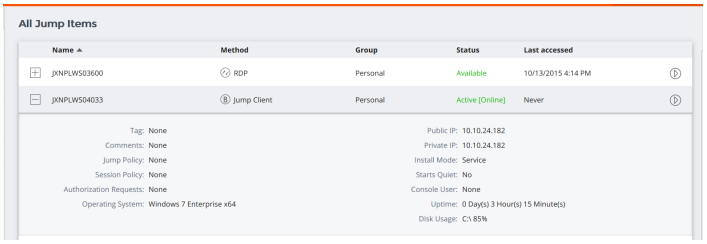
Gli elementi Jump sono raggruppati in base a chi può accedervi: solo l'utente che li ha creati o un particolare team. Ci sono tre modi per iniziare ad accedere agli endpoint:



- Individuare e selezionare un endpoint dall'elenco **Tutti gli elementi Jump**.
- Scegliere una coda del team e selezionare un endpoint dall'elenco di endpoint del team.
- Selezionare una sessione dall'elenco **Elementi Jump utilizzati di frequente**.

> ***Nota:*** *Nell'elenco* ***Elementi Jump utilizzati di frequente*** *vengono visualizzati tutti gli elementi Jump ai quali l'utente accede regolarmente. Per avviare una sessione con un elemento utilizzato di frequente, passare il mouse sulla sessione e fare clic su* ***Avvia una sessione****.*

Per avviare l'accesso agli elementi Jump, seguire i passaggi descritti di seguito:

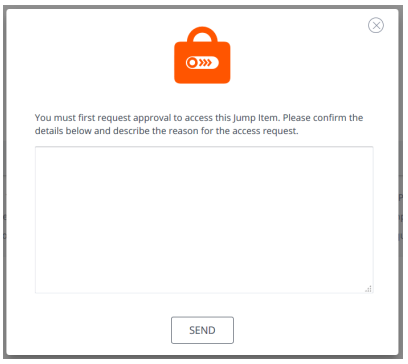


1. Selezionare una posizione e fare clic sul pulsante **Aggiorna tutto**.
2. Verrà visualizzato un elenco di tutti gli elementi Jump ed è possibile esaminare tutti i dettagli dell'elemento Jump, tra cui: **Nome**, **Metodo**, **Gruppo**, **Stato** e **Ultimo accesso**. Per esaminare maggiori dettagli sull'elemento Jump, fare clic sul segno + accanto al nome dell'elemento Jump.
3. Fai clic sul pulsante **Avvia** per iniziare una sessione con l'endpoint.

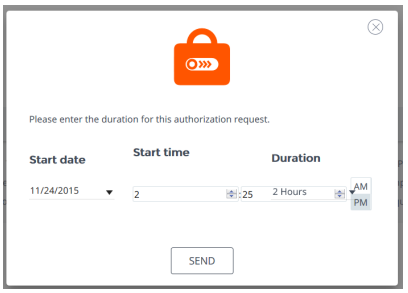
Autorizzazione dell'utente finale o di una terza parte

A seconda della configurazione degli elementi Jump all'interno dell'interfaccia amministrativa /login, un elemento Jump può avere una procedura Jump associata, e la procedura può definire il componente di autorizzazione che forza l'utente a richiedere l'autorizzazione da una terza parte o un amministratore prima di iniziare ad accedere alla sessione con l'elemento Jump. Per maggiori informazioni sulla configurazione delle notifiche e dell'approvazione di una terza parte e di un utente finale, consultare la sezione Procedure Jump: impostare pianificazioni, notifiche e approvazioni per gli elementi Jump.

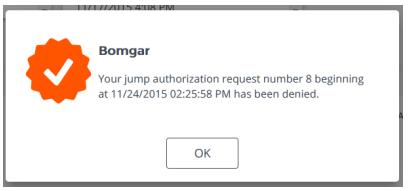
1. Dopo aver fatto clic sul pulsante **Avvia** e aver richiesto l'accesso, verrà chiesto all'utente di inserire il motivo della richiesta di accesso al sistema.



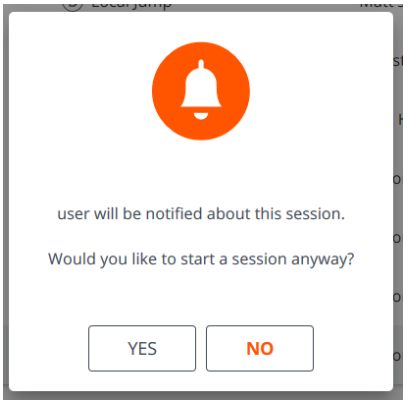
2. L'utente dovrà poi indicare quando e per quanto tempo vuole accedere al sistema.
3. Dopo aver inviato la richiesta, la terza parte o la persona responsabile dell'approvazione delle richieste di accesso saranno avvisati tramite una notifica via e-mail e avranno la possibilità di accettare o rifiutare la richiesta.



4. Dopo aver stabilito l'autorizzazione, verrà visualizzata la notifica di autorizzazione che mostra "approvata" o "rifiutata". Se viene concessa l'autorizzazione, l'utente può fare clic sul pulsante **OK** per iniziare l'accesso al sistema.

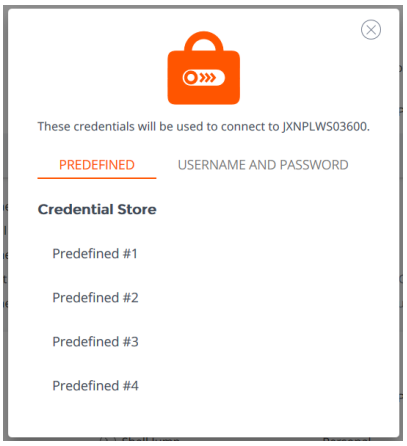


5. L'utente riceve un messaggio che chiede se desidera iniziare una sessione di accesso.
6. Se l'utente sceglie di iniziare la sessione, i commenti della parte che approva verranno visualizzati e l'utente può iniziare ad accedere al sistema.



Credenziali per la connessione automatica

Le credenziali del **Manager credenziali endpoint** si possono utilizzare per l'accesso RDP e per eseguire il Remote Push. Se un utente seleziona di eseguire il jump su un Jump remoto o su un elemento Jump RDP remoto e non è disponibile l'accesso automatico con credenziali, è necessario inserire un nome utente e la password nel prompt prima dell'inizio della sessione di accesso con l'endpoint. Se l'interfaccia amministrativa /login è stata configurata con l'accesso automatico con credenziali e restituisce un solo set di credenziali disponibili per un determinato utente ed elemento Jump, la richiesta di credenziali verrà saltata e saranno utilizzate le singole credenziali per avviare la sessione. Se è presente più di una credenziale configurata nell'interfaccia amministrativa /login, l'utente può scegliere nell'archivio delle credenziali oppure inserire le proprie credenziali manualmente. Per maggiori informazioni sulla configurazione e la gestione delle credenziali, consultare Sicurezza: Gestire le impostazioni di sicurezza all'indirizzo www.bomgar.com/docs/privileged-access/getting-started/admin/security.htm.



Accedere agli endpoint utilizzando l'inserimento delle credenziali

Quando si accede un elemento Jump basato su Windows dalla Console di accesso Privileged Web, è possibile utilizzare le credenziali di un archivio delle credenziali per accedere all'endpoint o per eseguire applicazioni come amministratore.

Prima di inserire le credenziali, accertarsi di disporre dell'archivio delle credenziali o la password per la connessione a Bomgar PAM.

Nota: *Non si dispone di una password vault? Maggiori informazioni su* ***Bomgar Vault*** *sono disponibili all'indirizzo https://www.bomgar.com/vault.*

Installare e configurare il Manager credenziali endpoint

Prima di iniziare ad accedere agli elementi Jump utilizzando l'inserimento delle credenziali, è necessario scaricare, installare e configurare il Manager credenziali endpoint Bomgar. Bomgar Manager credenziali endpoint consente di configurare rapidamente la connessione all'archivio delle credenziali, come ad esempio una password vault.

Nota: *Il Manager credenziali endpoint deve essere installato sul sistema per abilitare il servizio Bomgar Manager credenziali endpoint e utilizzare l'inserimento delle credenziali nel Bomgar PAM.*

Requisiti di sistema

- **Windows Vista o superiore, soltanto a 64 bit**
- **.NET 4.5 o superiore**

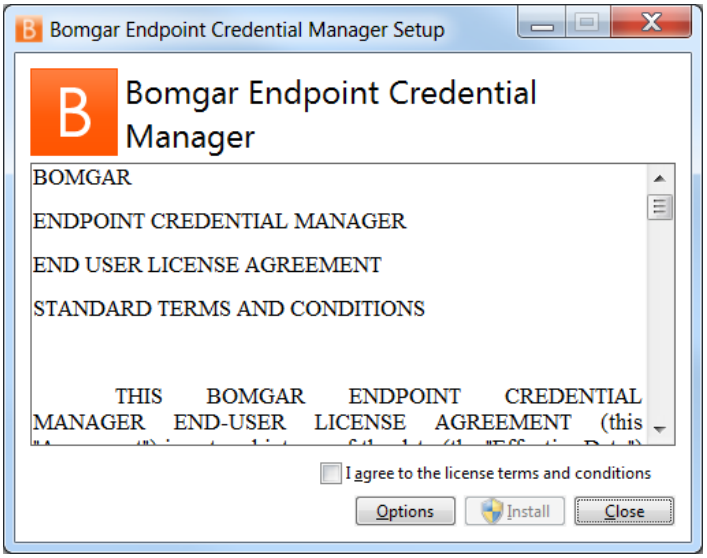
Nota: *Quando si installa il Manager credenziali endpoint per l'utilizzo con Bomgar Vault, si consiglia di installarlo su una macchina con un indirizzo IP statico per evitare potenziali problemi con il whitelisting dell'IP di Vault per l'API.*

1. Per iniziare scaricare **Bomgar Manager credenziali endpoint** da Supporto tecnico Bomgar all'indirizzo https://help.bomgar.com/. Avviare la **Procedura guidata alla configurazione di Bomgar Manager credenziali endpoint**.

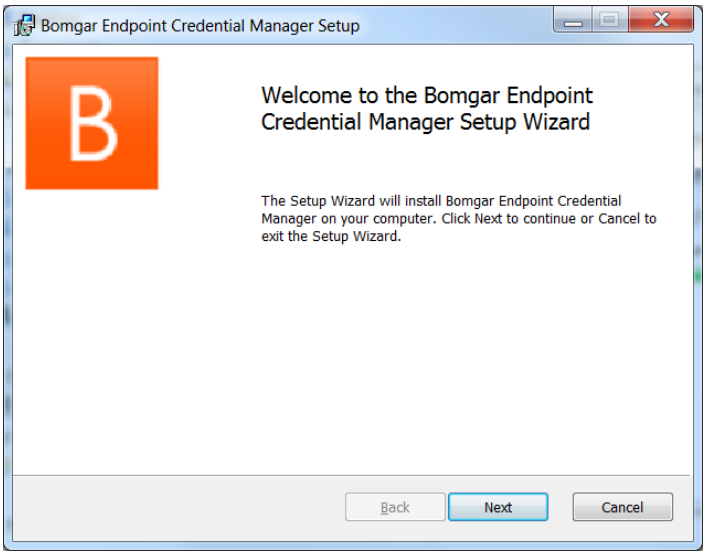
2. Dare il consenso ai termini e alle condizioni dell'EULA. Selezionare la casella di controllo e fare clic su **Installa**.

   Nota: *Non è consentito procedere con l'installazione se non si è dato prima il consenso all'EULA.*

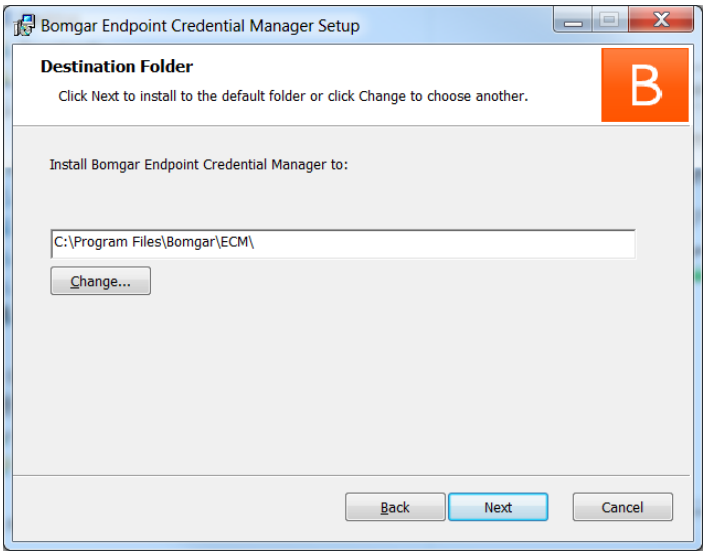
   Fare clic sul pulsante **Opzioni** per personalizzare la configurazione di installazione.



3. Fare clic su **Avanti**.



4. Scegliere una posizione per il Manager delle credenziali e fare clic su **Avanti**.
5. Nella schermata successiva, è possibile iniziare l'installazione o rivedere un passaggio precedente.
6. Quando si è pronti a iniziare fare clic su **Installa**.
7. L'installazione richiede qualche minuto. Nella schermata, fare clic su **Fine**.



Configurare una connessione nell'archivio delle credenziali

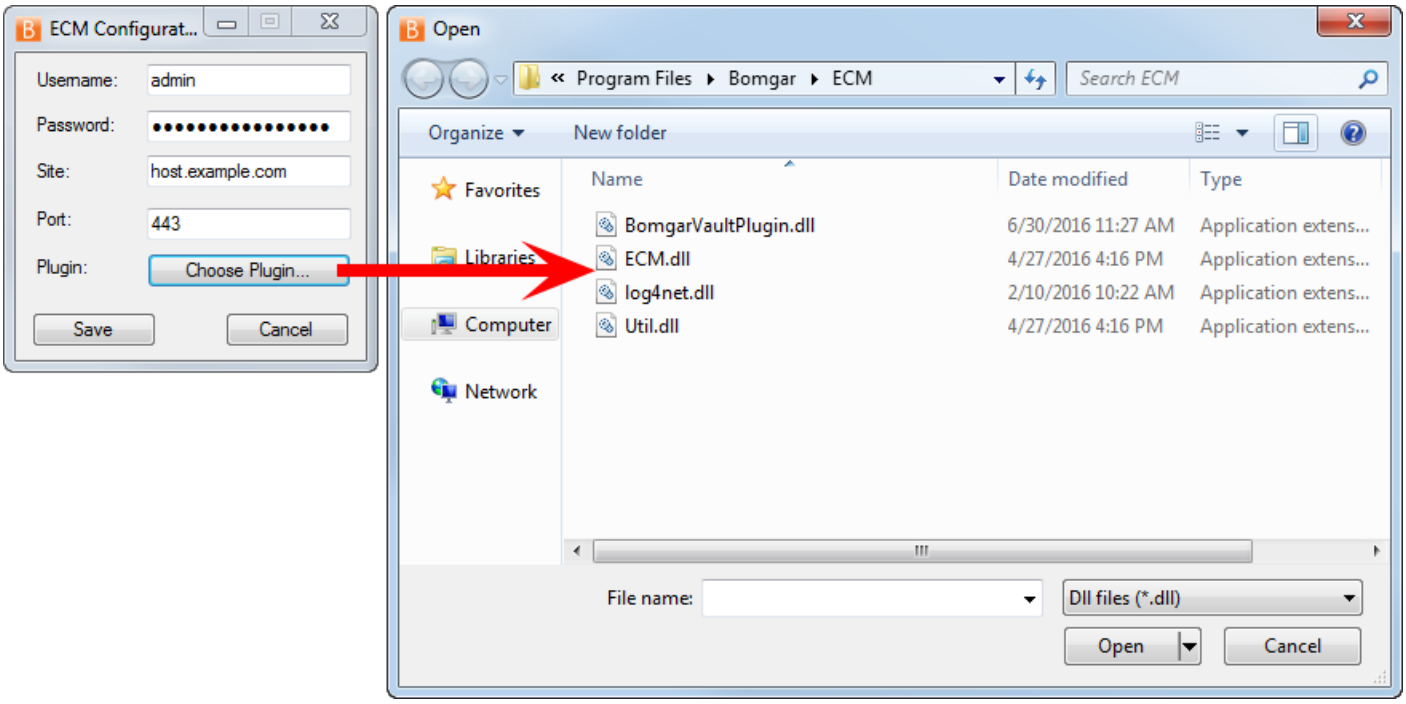
Utilizzare il configuratore del Manager credenziali endpoint, impostare una connessione nell'archivio delle credenziali.

1. Individuare il configuratore di Manager credenziali endpoint appena installato utilizzando Windows Search oppure visualizzando l'elenco dei programmi del menu Start.
2. Eseguire il programma per iniziare a stabilire la connessione.
3. Quando il configuratore del Manager credenziali endpoint si apre completare i campi. Tutti i campi sono obbligatori.

Inserire i valori seguenti:

Etichetta del campo	**Valore**
Nome utente	Il nome utente Admin dell'archivio delle credenziali.
Password	La password Admin dell'archivio delle credenziali.
Sito	L'URL dell'istanza dell'archivio delle credenziali.
Porta	La porta del server mediante il quale il Manager credenziali endpoint si connette al sito dell'utente.
Plugin	Fare clic sul pulsante **Scegli plugin...** per individuare il plugin.

4. Quando fai clic sul pulsante **Scegli plugin...**, si apre la cartella del Manager credenziali endpoint.
5. Incollare i file di plugin nella cartella.
6. Aprire il file del plugin per iniziare il caricamento.



Nota: *Se ci si sta collegando a una password vault, potrebbe essere necessaria una ulteriore configurazione a livello di plugin. I requisiti del plugin possono variare in base all'archivio delle credenziali alle quali si è connessi.*

IMPORTANTE

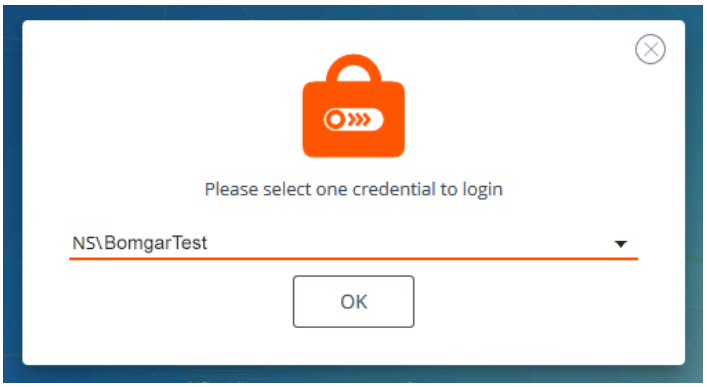
Per applicare le nuove impostazione nella configurazione riavviare il servizio Manager credenziali endpoint.

Utilizzare l'inserimento delle credenziali per accedere agli endpoint

Dopo aver configurato l'archivio delle credenziali e aver stabilito la connessione, la Console di accesso Privileged Web può iniziare a utilizzare le credenziali nell'archivio delle credenziali per accedere agli endpoint.

1. Accedere alla Console di accesso Privileged Web.
2. Eseguire il Jump su un endpoint con un elemento Jump installato come servizio elevato su una macchina Windows.
3. Fare clic sul pulsante **Riproduci** per iniziare la condivisione schermo con l'endpoint. Se l'endpoint è nella schermata di accesso Windows, il pulsante **Inserisci credenziali** è evidenziato.
4. Fare clic sul pulsante **Inserisci credenziali**. Viene visualizzata una finestra di dialogo per la selezione delle credenziali con l'elenco delle credenziali disponibili in Manager credenziali endpoint.

5. Selezionare le credenziali appropriate da utilizzare dal Manager credenziali endpoint. Il sistema recupera le credenziali dal Manager credenziali endpoint e le inserisce nella schermata di accesso Windows.
6. L'utente è connesso all'endpoint.



Autenticazione dall'URL dell'API dello script del client

Questa funzione consente agli utenti di accedere alla console di accesso Privileged Web e di eseguire il Jump a un endpoint utilizzando l'API dello script del client PAM (https://www.bomgar.com/docs/privileged-access/how-to/integrations/api/client-script/index.htm#client-scripting-api).

L'URL dell'API dello script del client segue il formato **https://access.example.com/api/client_script**, dove access.example.com è il nome host del dispositivo.

Questa API accetta un tipo di client (**web_console**), un'operazione da eseguire (**execute**) e un comando (**start_jump_item_session**). Non è supportato alcun altro comando per il tipo di client **web_console**.

Se l'utente è connesso alla console di accesso desktop quando all'URL dell'API dello script del client si accede con **type=web_console**, l'utente accede alla console di accesso Privileged Web e viene disconnesso dalla console di accesso desktop. Se questo comportamento non è desiderato, l'utente deve utilizzare un URL dell'API dello script del client con **type=rep** invece di **type=web_console**.

Se invece l'utente è connesso alla console di accesso Privileged Web e l'API chiama **type=rep**, l'utente accede alla console di accesso desktop e viene disconnesso dalla console di accesso Privileged Web.

Di seguito viene riportato un esempio di richiesta API dello script del client:

```
https://access.example.com/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEFG02
```

Se l'utente è già connesso alla console di accesso Privileged Web e la richiesta precedente esegue il comando nella scheda del browser che esegue la console di accesso Privileged Web. In questo caso, il comando avvia una sessione con il Jump Client il cui nome host, commenti, IP pubblico o IP privato corrispondono alla stringa di ricerca "ABCDEF02".

Se l'utente non è già connesso alla console di accesso Privileged Web e la richiesta precedente apre una nuova scheda Browser e indirizza l'utente a /login per l'autenticazione (questo passaggio viene saltato se l'utente è già connesso a /login). L'utente viene quindi reindirizzato alla console di accesso Privileged Web e il comando avvia una sessione con il Jump Client il cui nome host, commenti, IP pubblico o IP privato corrispondono alla stringa di ricerca "ABCDEF02".

In entrambi i casi se più di un elemento Jump corrisponde ai criteri di ricerca, l'utente deve selezionare l'elemento Jump corretto dall'elenco. Se nessun elemento Jump corrisponde ai criteri di ricerca, la console di accesso Web visualizza un messaggio di errore all'utente.

Tutti i criteri di ricerca per il comando **start_jump_item_session** sono supportati con **type=web_console**, tra cui:

- jump.method
- search_string
- client.hostname
- client.comments
- client.tag
- client.public_ip
- client.private_ip
- session.custom.<attribute code name>

Tornare a una sessione attiva nella Console di accesso Privileged Web

Se sono in corso più sessioni di accesso, è possibile tornare a un'altra sessione di accesso in qualsiasi momento. Per tornare a un endpoint al quale si è connessi in un'altra sessione, seguire i passaggi definiti di seguito:

1. Fare clic sul menu a discesa **Sessioni**.

> ***Nota:*** *Il numero elencato nel menu a discesa* ***Sessioni*** *indica il numero di sessioni alle quali si accede simultaneamente.*

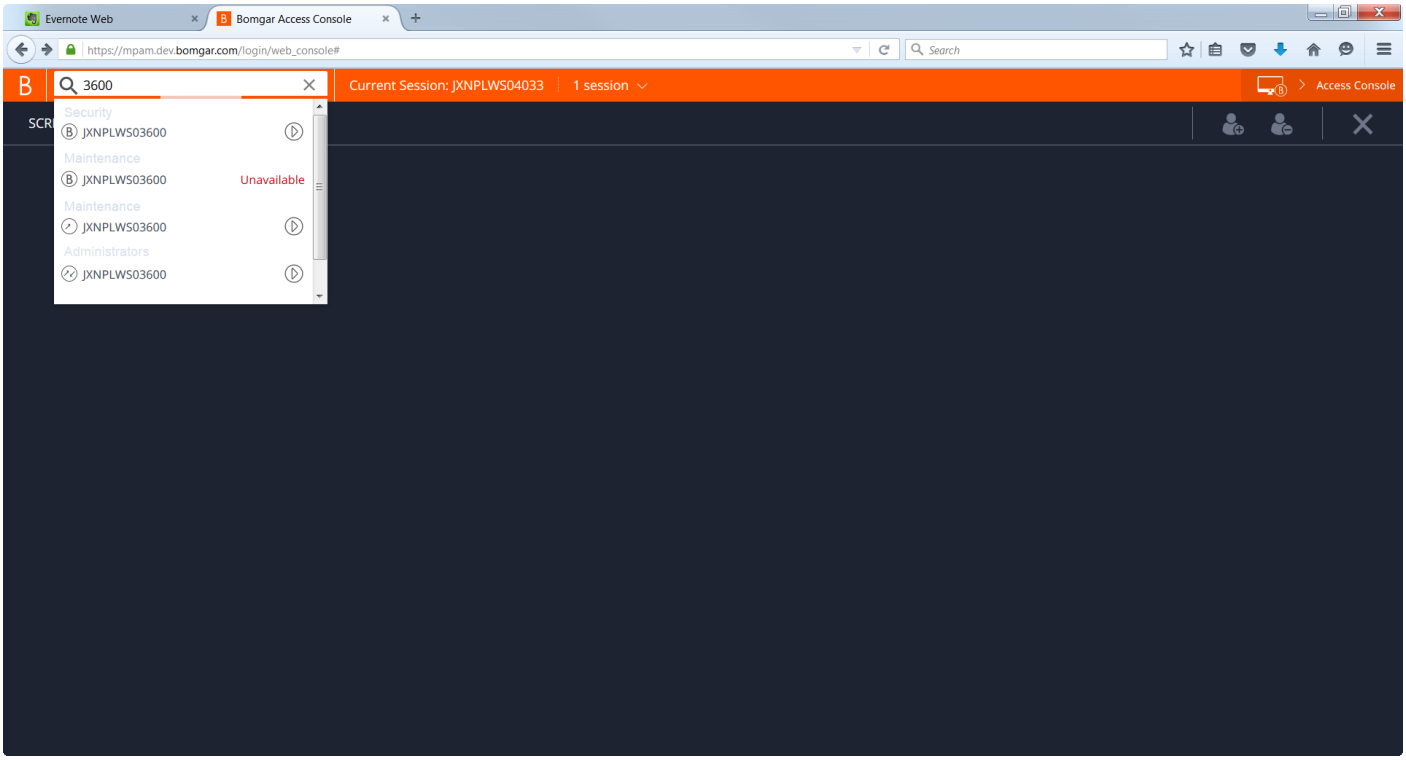
2. Selezionare un endpoint dall'elenco.

3. L'utente viene indirizzato alla sessione dell'endpoint specificato.

Cerca endpoint

Quando si utilizza la Console di accesso Privileged Web è possibile cercare endpoint specifici durante una sessione di accesso. Nei risultati di ricerca è possibile anche fare clic sul pulsante **Avvia** per iniziare una sessione con quell'endpoint.

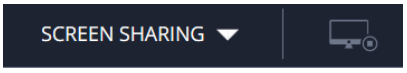
1. Fare clic sull'icona **Cerca** presente nella parte superiore dello schermo.
2. Nella barra di ricerca, digitare il nome dell'endpoint.
3. Tra i risultati forniti selezionare l'endpoint con il quale iniziare una sessione e fare clic sul pulsante **Avvia** per iniziare una sessione.



Controllo dell'endpoint remoto con la condivisione dello schermo

Per visualizzare e controllare i sistemi remoti, utilizzare l'azione di condivisione schermo durante una sessione di accesso.

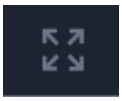
1. Da questa finestra di sessione fare clic sul menu a discesa **Condivisione schermo** e scegliere l'opzione **Condivisione schermo**. Oppure è possibile fare clic sull'icona **Avvia Condivisione schermo** per iniziare l'accesso all'endpoint.



2. Utilizzare una delle azioni seguenti durante una sessione per eseguire funzioni diverse.

Strumenti di Condivisione schermo

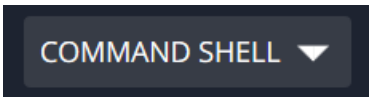
	Interrompi Condivisione schermo.
	Durante la visualizzazione del computer remoto, avviare o arrestare il controllo della tastiera e del mouse remoto.
	Se le autorizzazioni lo consentono, è possibile disabilitare la visualizzazione dello schermo e l'input del mouse e della tastiera dell'utente remoto. La vista dell'utente finale dello schermo privacy spiega chiaramente che l'utente Bomgar ha disattivato la vista dell'utente. L'utente finale può ripristinare il controllo in qualsiasi momento premendo **Ctrl-Alt-Canc**. Questa funzione è disponibile solo per i computer Windows. Per Vista e sistemi operativi successivi è necessario elevare l'endpoint del cliente. In Windows 8 e superiore, questa funzione è limitata alla disabilitazione del mouse e della tastiera.
	Riavviare il sistema remoto in modalità normale o provvisoria con funzionalità di rete oppure arrestare il sistema remoto.
	Consente di inviare un comando **Ctrl-Alt-Canc** al computer remoto.
	Eseguire un'operazione particolare sul sistema remoto. Le operazioni disponibili variano a seconda del sistema operativo e della configurazione del computer remoto. Gli script preconfezionati sono disponibili per l'utente nel menu a comparsa. L'azione speciale Esegui come un sistema Windows® consente di selezionare le credenziali da un Manager credenziali endpoint. 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.
	Consente di attivare/disattivare la tastiera virtuale.

	Consente di selezionare un monitor remoto alternativo da visualizzare. Il monitor primario è contrassegnato da una **P**.
	Consente di visualizzare lo schermo remoto nelle dimensioni reali o scalarmente ridotte.
	Selezionare la modalità di ottimizzazione del colore per la visualizzazione dello schermo remoto. Se si condivide soprattutto il video, selezionare **Video ottimizzato**; in caso contrario selezionare tra **Bianco e nero** (utilizza meno larghezza di banda), **Pochi colori**, **Altri colori** o **Tutto colore** (utilizza più larghezza di banda).
	Consente di visualizzare il desktop remoto in modalità schermo intero o tornare alla visualizzazione di interfaccia. Nella modalità schermo intero, vengono passate chiavi speciali al sistema remoto. Questo include, ma non si limita a tasti di modifica, tasti funzione e il pulsante Start di Windows. Tenere presente che non si applica al comando **Ctrl-Alt-Canc**.

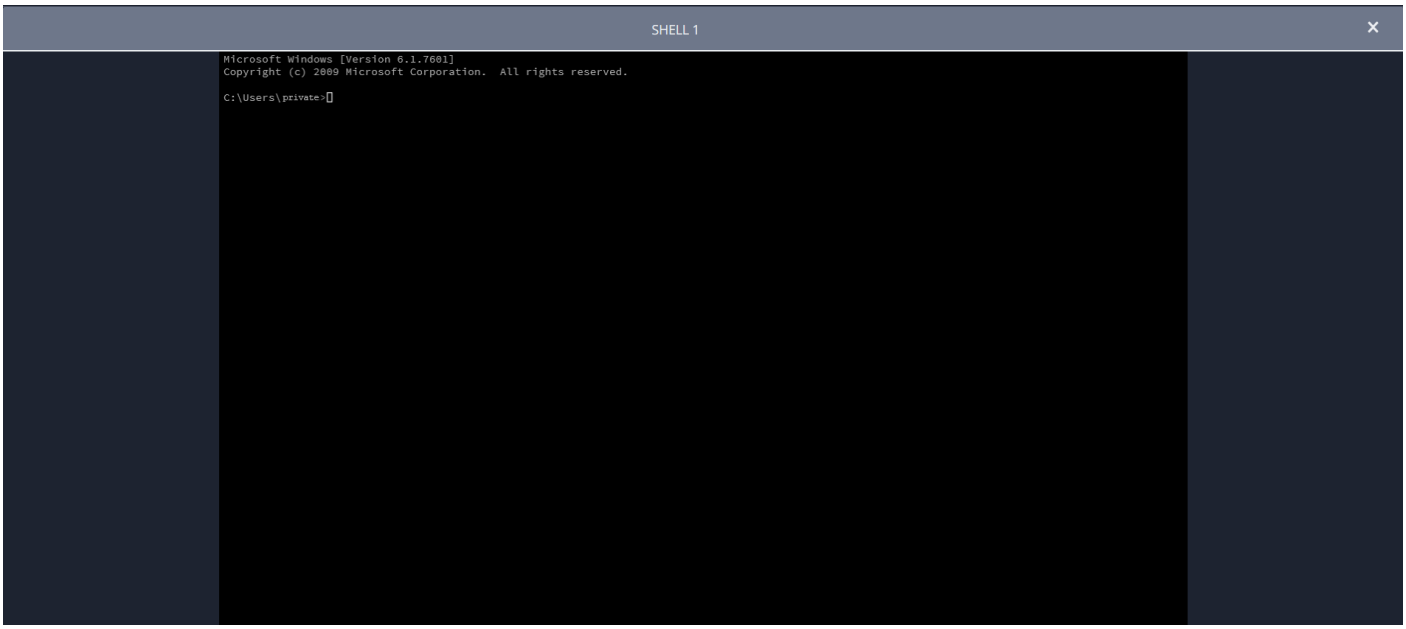
Accedere alla shell di comando sull'endpoint remoto

La shell di comando remota consente all'utente con i necessari privilegi di aprire un'interfaccia virtuale della riga di comando nel sistema remoto. In tal modo l'utente può eseguire la digitazione nel proprio computer e ottenere che i comandi siano eseguiti nel sistema remoto. Il tecnico di supporto può lavorare con più shell di comando. Tenere presente che gli script disponibili per l'utente possono essere eseguiti anche sul sistema remoto dall'interfaccia di condivisione schermo.

L'amministratore può anche attivare la registrazione di shell remote in modo che successivamente, nel report della sessione, si possa vedere un filmato di ogni shell. Se è attivata la registrazione della shell, sarà inoltre disponibile la trascrizione della shell di comando.



1. Per accedere alla **Shell di comando** durante una sessione di accesso, fare clic sul menu a discesa **Condivisione schermo** nell'angolo in alto dello schermo.
2. Selezionare l'opzione **Shell di comando**.
3. Dopo aver selezionato l'opzione **Shell di comando**, vengono visualizzate le opzioni e il prompt di comando.



Strumenti della shell di comando

	Interrompi accesso al prompt di comando quando non è più necessario.
	Aprire una nuova shell per eseguire diversi prompt di comando oppure chiudere le singole shell senza rinunciare all'accesso al prompt di comando. Le shell sono classificate in fondo allo schermo.

Condivisione di una sessione con altri utenti che utilizzano la Console di accesso Privileged Web

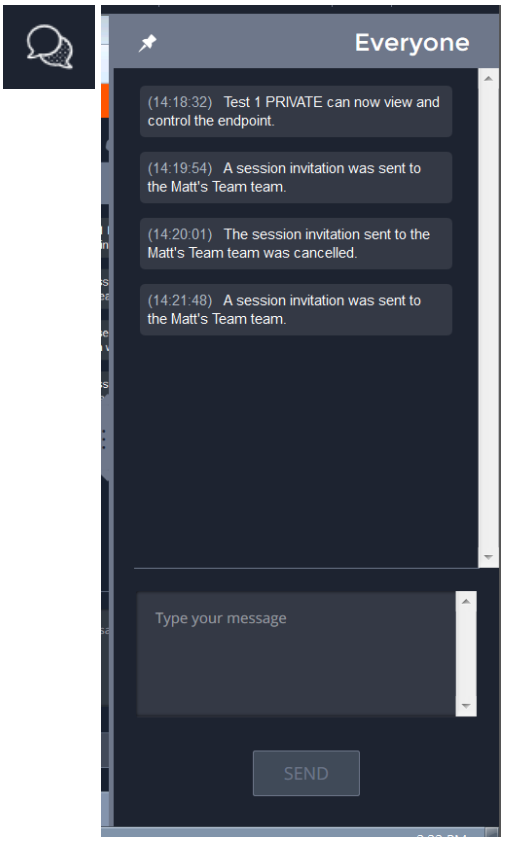
In una sessione è possibile richiedere al membro del team di partecipare a una sessione di accesso. Per condividere una sessione, seguire i passaggi descritti di seguito.

1. Fare clic sull'icona **Condividi sessione**.

2. Selezionare dal menu il team di cui l'utente è membro.

3. Dall'elenco del team scegliere l'utente con cui si desidera condividere la sessione.

4. Una volta che l'utente è entrato nella sessione, è possibile chattare facendo clic sull'icona **Chat** nella parte superiore dello schermo



Si possono inviare più inviti per far partecipare più utenti alla sessione. Gli utenti sono elencati solo quando sono connessi alla console di accesso o se hanno la modalità Disponibilità estesa attivata.

Se è consentito condividere sessioni con gli utenti che non sono membri dei propri team, vengono visualizzati anche altri team a condizione che comprendano almeno un membro connesso alla console di accesso o con la modalità Disponibilità estesa attivata.

Solo il titolare della sessione può inviare inviti. Gli inviti non scadono fino a quando si rimane titolari della sessione. Un utente non può avere più inviti attivi a partecipare alla stessa sessione. L'invito scompare se:

- L'utente che ha esteso l'invito lo annulla.
- L'utente che invita lascia la sessione.
- La sessione termina.
- L'utente invitato accetta l'invito.

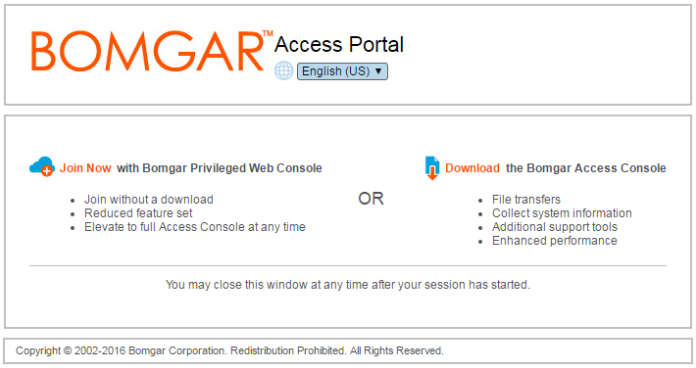
.

Invitare un utente esterno a partecipare a una sessione

In una sessione un utente può chiedere a un utente esterno di partecipare una tantum a una sessione. Per invitare un utente esterno a una sessione, seguire i passaggi descritti di seguito.

1. In una sessione, fare clic sul pulsante **Condividi sessione**.
2. Dal menu, selezionare **Invita tecnico di supporto esterno**.
3. Selezionare una procedura di sicurezza. Queste procedure vengono create nell'interfaccia amministrativa /login e determinano il livello di autorizzazione del tecnico di supporto esterno. Quando si seleziona un profilo, subito sotto ne viene visualizzata la descrizione completa.
4. Immettere il nome dell'utente invitato. Questo nome viene visualizzato nella finestra di chat e nei report.
5. Inserire quindi commenti sul motivo dell'invito di questo utente.

6. Fare clic su **Invia**, viene visualizzata un'altra finestra di dialogo con l'URL di invito.
7. A seconda delle opzioni selezionate dall'amministratore, è possibile inviare l'invito dall'e-mail locale da un server della posta. Si può inoltre copiare e incollare l'URL diretto e inviarlo all'utente.
8. Quando l'utente esterno fa clic sull'URL di invito all'accesso, ha la possibilità di partecipare alla sessione utilizzando la console di accesso Privileged Web o scaricare e installare la console di accesso desktop.
9. Una volta selezionata la console di accesso Privileged Web o installata la console di accesso desktop, è possibile partecipare alla sessione.



Nota: *Ecco alcuni suggerimenti per l'utilizzo della funzione di invito di un utente esterno:*

- *L'utente esterno ha accesso solo alla scheda di sessione e dispone di una serie limitata di privilegi.*
- *L'utente esterno non può mai essere il titolare della sessione.*
- *Quando l'utente che invita lascia la sessione, l'utente esterno viene disconnesso.*
- *L'utente può invitare più di un utente esterno.*
- *L'utente esterno può elevare alla Console di accesso desktop. Quando il pulsante **Eleva** è selezionato, si apre una nuova scheda del browser che reindirizza l'utente all'URL di invito all'accesso per la Console di accesso desktop.*

Rimuovere un membro da una sessione della Console di accesso Privileged Web

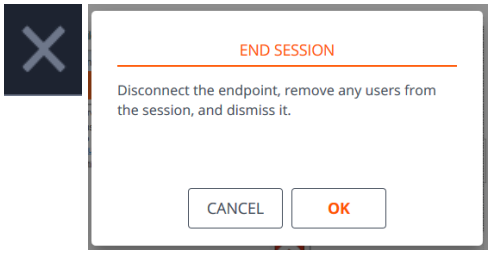
Se necessario, è possibile rimuovere un altro utente da una sessione condivisa. Per rimuovere un utente, fare clic sull'icona **Rimuovi membro**.

Dal menu selezionare il partecipante da rimuovere. Fare clic su **Rimuovi membro**.

> ***Nota:*** *È necessario essere il titolare della sessione per rimuovere un altro membro.*

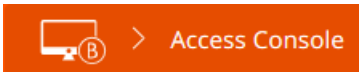
Chiudi sessione della Console di accesso Privileged Web

1. Per uscire dalla sessione di accesso fare clic sull'icona **X** nell'angolo in alto a destra dello schermo. Se si è titolari della sessione, tenere presente che l'azione **Fine sessione** chiude la pagina della sessione nella console di accesso e rimuove gli altri membri che condividono la sessione.
2. Successivamente si riceve un prompt che chiede se si desidera terminare la sessione.
3. Se si fa clic su **OK**, la sessione termina, e si viene reindirizzati all'elenco **Tutti gli elementi Jump**.



Scaricare il desktop nativo dalla Console di accesso Privileged Web

Quando si utilizza la Console di accesso Privileged Web, è possibile scegliere in qualsiasi momento di scaricare la console di accesso nativa del desktop sul computer.



1. Per scaricare la console di accesso nativa del desktop dalla Console di accesso Privileged Web, fare clic sul pulsante **Esegui console di accesso nativa** presente nell'angolo in altro a destra dello schermo.
2. Quando appare la procedura guidata d'installazione, segui le istruzioni per installare il software.

Nota: *in un sistema Linux, è necessario salvare il file nel proprio computer e poi aprirlo dalla posizione in cui è stato scaricato. Non servirsi del link Apri che appare dopo avere scaricato il file con alcuni browser.*