

**BOMGAR™**

**Privileged Access Management  
Privileged Web**

## Indice

---

<b>Guida a Privileged Web</b> .....	<b>3</b>
Requisiti Privileged Web .....	4
Avvia Privileged Web mediante /login .....	5
Utilizzare gli elementi Jump per accedere agli endpoint nel Privileged Web .....	7
Tornare a una sessione attiva in Privileged Web .....	10
Controllo dell'endpoint remoto con la condivisione dello schermo .....	11
Accedere alla shell di comando sull'endpoint remoto .....	13
Condivisione di una sessione con altri utenti che utilizzano il Privileged Web .....	14
Rimuovere un membro da una sessione Privileged Web .....	16
Chiudi sessione Privileged Web .....	17
Scaricare il desktop nativo da Privileged Web .....	18

## Guida a Privileged Web

Grazie a Privileged Web di 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 il 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](http://help.bomgar.com).

## Requisiti Privileged Web

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

### Piattaforme

- Windows
- Macintosh
- Linux

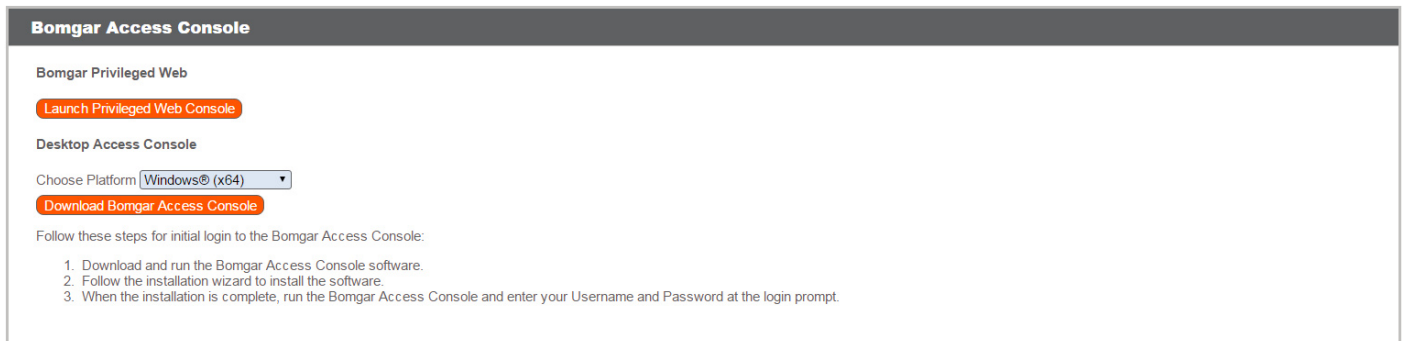
### Browser

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

## Avvia Privileged Web mediante /login

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 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 Web** presente nella sezione **Console di accesso Bomgar**.
6. Si apre la console di accesso Web nella nuova scheda ed è possibile iniziare ad accedere agli endpoint.

B Q Access Console

- All Jump Items
- Personal
- Team: Administrators
- Team: Maintenance
- Team: Security

### Frequently Used Jump Items

REFRESH ALL

#### All Jump Items

Name ▲	Method	Group	Status	Last accessed	
<span style="border: 1px solid #ccc; padding: 2px;">+</span> IE11WIN7	<span style="border: 1px solid #ccc; padding: 2px;">B</span> Jump Client	Security	Passive [Unknown]	Never	<span style="border: 1px solid #ccc; padding: 2px;">D</span>
<span style="border: 1px solid #ccc; padding: 2px;">+</span> judges	<span style="border: 1px solid #ccc; padding: 2px;">S</span> Shell Jump	Administrators	Available	11/20/2015 3:57 PM	<span style="border: 1px solid #ccc; padding: 2px;">D</span>
<span style="border: 1px solid #ccc; padding: 2px;">+</span> JXNPLWS03600	<span style="border: 1px solid #ccc; padding: 2px;">B</span> Jump Client	Maintenance	Active [Online]	11/20/2015 3:51 PM	<span style="border: 1px solid #ccc; padding: 2px;">D</span>
<span style="border: 1px solid #ccc; padding: 2px;">+</span> JXNPLWS03600	<span style="border: 1px solid #ccc; padding: 2px;">B</span> Local Jump	Security	Unavailable	Never	<span style="border: 1px solid #ccc; padding: 2px;">D</span>
<span style="border: 1px solid #ccc; padding: 2px;">+</span> JXNPLWS03600	<span style="border: 1px solid #ccc; padding: 2px;">R</span> Remote Jump	Maintenance	Available	11/17/2015 4:08 PM	<span style="border: 1px solid #ccc; padding: 2px;">D</span>
<span style="border: 1px solid #ccc; padding: 2px;">+</span> JXNPLWS03600	<span style="border: 1px solid #ccc; padding: 2px;">R</span> RDP	Administrators	Available	11/10/2015 8:59 AM	<span style="border: 1px solid #ccc; padding: 2px;">D</span>

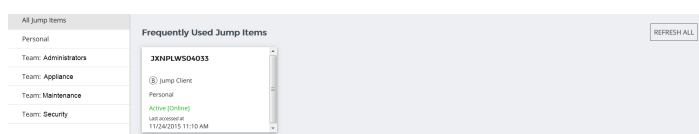
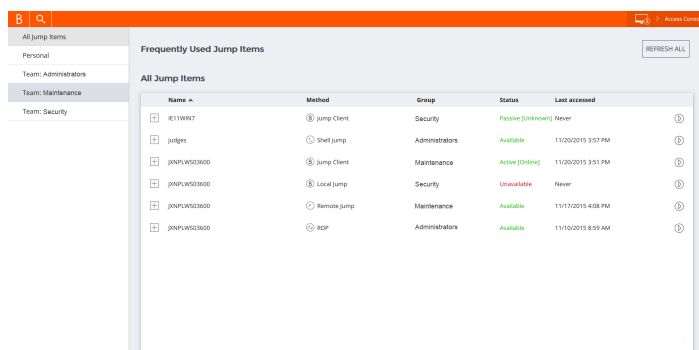
## Utilizzare gli elementi Jump per accedere agli endpoint nel Privileged Web

Per accedere a un endpoint, installare un elemento Jump sul sistema dalla pagina dei **Jump Clients** dell'interfaccia amministrativa di /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:

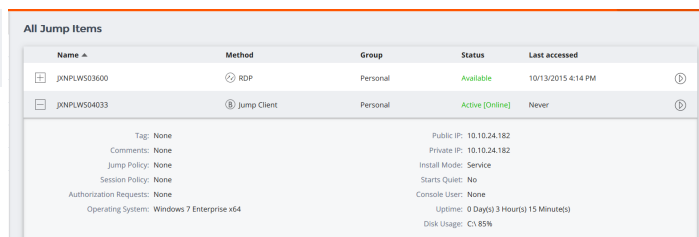
- Individuare e selezionare un endpoint dall'elenco **Tutti gli elementi Jump**.
- Scegliere una coda del team e selezionare un endpoint dall'elenco di endpoint del team.
- Selezionare una sessione dall'elenco **Elementi Jump utilizzati di frequente**.



**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:

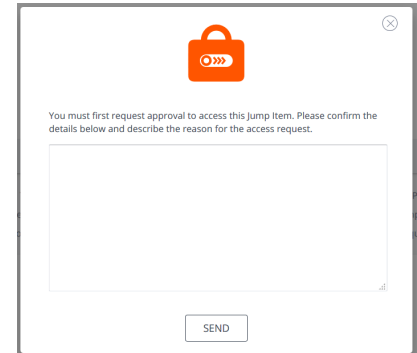
1. Selezionare una posizione e fare clic sul pulsante **Aggiorna tutto**.
2. Verrà visualizzato un elenco di tutti gli elementi Jump ed è possibile esaminare tutti i dettagli dell'elemento Jump, tra cui: **Nome, Metodo, Gruppo, Stato e Ultimo accesso**. Per esaminare maggiori dettagli sull'elemento Jump, 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 [Procedura Jump: impostare pianificazioni, notifiche e approvazioni per gli elementi Jump](#).

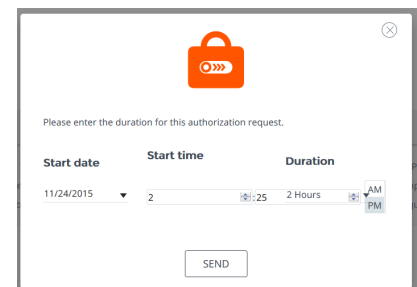
1. Dopo aver fatto clic sul pulsante **Avvia** e aver richiesto l'accesso, verrà chiesto all'utente di inserire il motivo della richiesta di accesso al sistema.
2. L'utente dovrà poi indicare quando e per quanto tempo vuole accedere al sistema.
3. Dopo aver inviato la richiesta, la terza parte o la persona 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.




11/24/2015 4:38 PM



You must first request approval to access this jump item. Please confirm the details below and describe the reason for the access request.

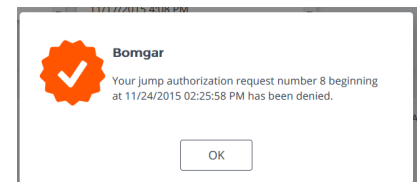


11/24/2015 4:38 PM




Please enter the duration for this authorization request.

Start date	Start time	Duration
11/24/2015	2:25	2 Hours

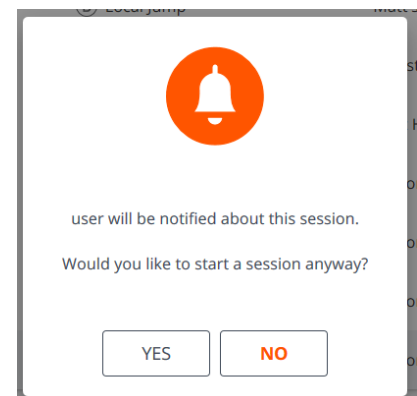


11/24/2015 4:38 PM




**Bomgar**

Your jump authorization request number 8 beginning at 11/24/2015 02:25:58 PM has been denied.



11/24/2015 4:38 PM



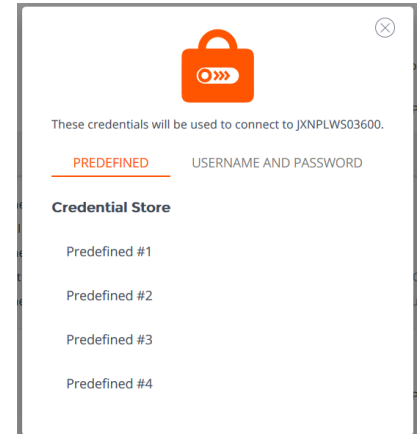
user will be notified about this session.

Would you like to start a session anyway?



### 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](#).



## Tornare a una sessione attiva in 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.

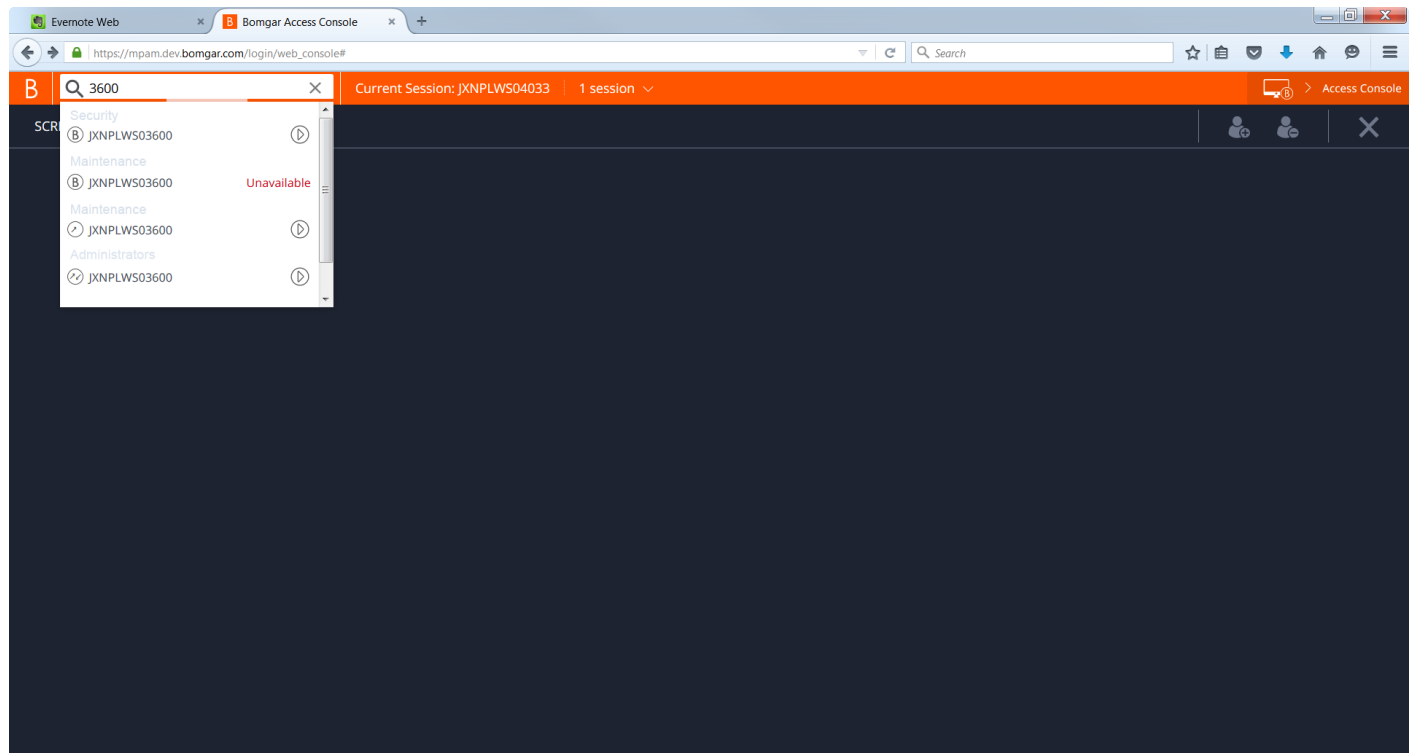
2. Selezionare un endpoint dall'elenco.
3. L'utente viene indirizzato alla sessione dell'endpoint specificato.



### Cerca endpoint

Quando si utilizza 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.

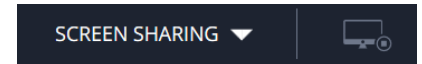
1. Fare clic sull'icona **Cerca** presente nella parte superiore dello schermo.
2. Nella barra di ricerca, digitare il nome dell'endpoint.
3. Tra i risultati forniti selezionare l'endpoint con il quale iniziare una sessione e fare clic sul pulsante **Avvia** per iniziare una sessione.



## 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.



Questa funzione è disponibile solo per i computer Windows.



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.



Consente di attivare/disattivare la tastiera virtuale.



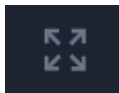
Consente di selezionare un monitor remoto alternativo da visualizzare. Il monitor primario è contrassegnato da una **P**.



Consente di visualizzare lo schermo remoto nelle dimensioni reali o scalarmente ridotte.



Consente di visualizzare lo schermo remoto in scala di grigi a 2 bit per il minimo consumo di ampiezza di banda, a colori a 8 bit per prestazioni veloci, a 16 bit per una qualità delle immagini e prestazioni medie o a 32 bit per la risoluzione delle immagini più alta.



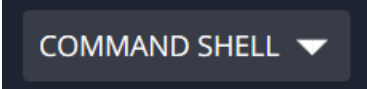
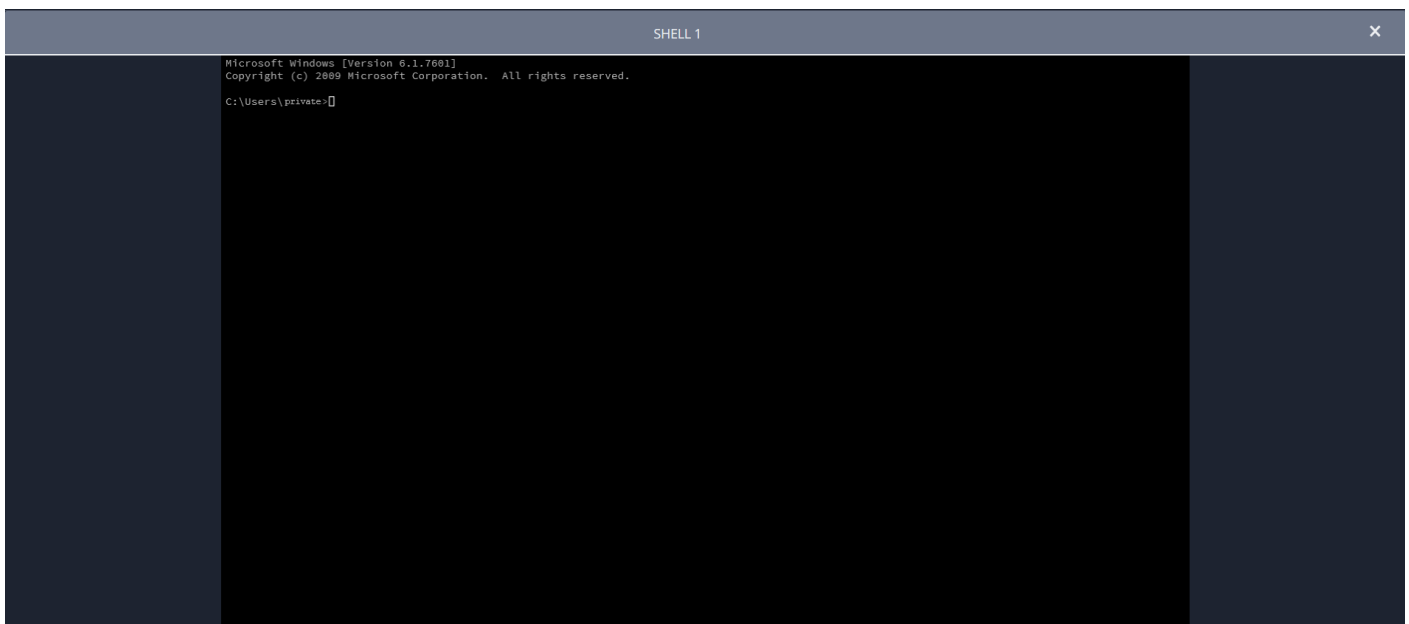
Consente di visualizzare il desktop remoto in modalità schermo intero o tornare alla visualizzazione di interfaccia. Nella modalità schermo intero, vengono passate chiavi speciali al sistema remoto. Questo include, ma non si limita a tasti di modifica, tasti funzione e il pulsante Start di Windows. Tenere 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.

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.

A dark grey rectangular button with the text 'COMMAND SHELL' in white uppercase letters and a white downward-pointing triangle on the right side.

## 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.

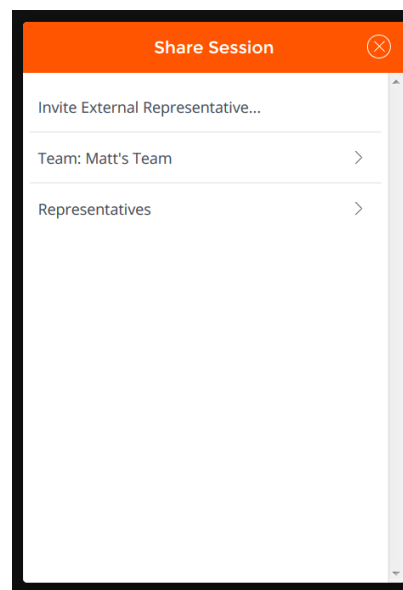
## Condivisione di una sessione con altri utenti che utilizzano il Privileged Web

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.

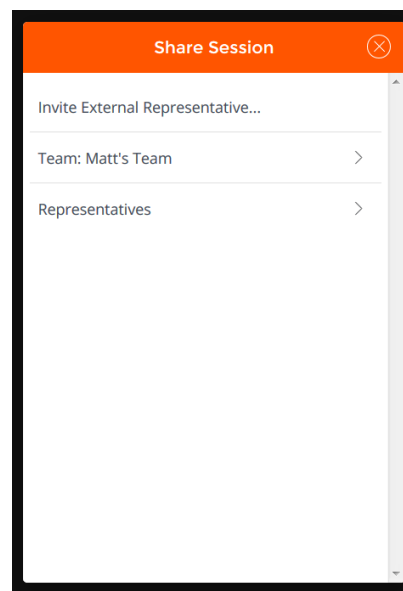
1. Fare clic sull'icona **Condividi sessione**.



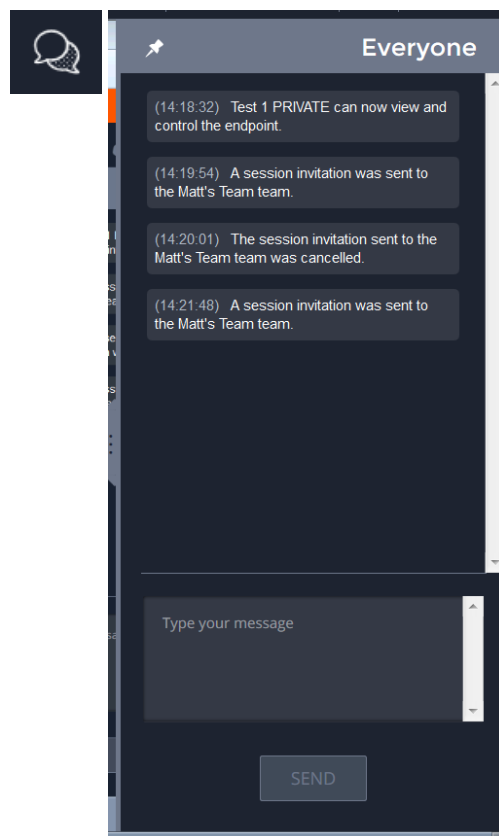
2. Selezionare dal menu il team di cui l'utente è membro.



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.

## Rimuovere un membro da una sessione Privileged Web

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



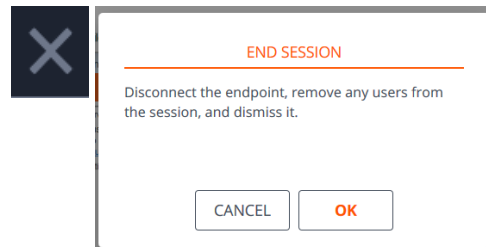
Dal menu selezionare il partecipante da rimuovere. Fare clic su **Rimuovi membro**.

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



## Chiudi sessione 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 da Privileged Web

Quando si utilizza 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 da Privileged Web, fare clic sul pulsante **Esegui console di accesso nativa** presente nell'angolo in alto 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.

