

BOMGAR™

**What's New in Bomgar Privileged
Access Management 15.3**

Table of Contents

Updates for Administrators	3
Endpoint Surface Analyzer	4
Jumpoint Management	5
Mass Import of Endpoints	6
Session Forensics	7
Updates for Users	8
Bomgar Privileged Web	9
Change Management Workflow	10
Linux Service Mode Jump Client	11
Mobile Access Console Enhancements	12
Multifactor Authentication	13

Updates for Administrators

Bomgar Privileged Access Management 15.3 contains the following updates for Bomgar administrators.

Feature
Endpoint Surface Analyzer Know and control how critical endpoints are accessed throughout your organization. Be aware of the listening network port exposure for systems that you manage. Report and keep a running log of critical endpoint network exposure.
Jumpoint Management Better manage your installed Jumpoints. Jumpoint information on /login now includes the host system's public and private IP addresses, hostname, and comments. Easily redeploy a Jumpoint to a new host, with the new Jumpoint replacing the old one for any existing Jump shortcuts associated with it. Jumpoints can be clustered to provide redundancy and additional load capacity for critical network segments. Additionally, Jumpoints no longer require a user to be assigned to them directly.
Mass Import of Endpoints When creating a large number of Jump shortcuts, you can import them via a spreadsheet in the /login interface or via the API. Importing Jump Items saves time and effort over manually adding each one in the access console.
Session Forensics Command shell recordings are now included in Session Forensics searches. Successful matches in stored shell recordings automatically take the user to that point in time in the recording.

Endpoint Surface Analyzer

Know and control how critical endpoints are accessed throughout your organization. Be aware of the listening network port exposure for systems that you manage. Report and keep a running log of critical endpoint network exposure.

Endpoint Analyzer Configuration

Enable Endpoint Analyzer

Enter the ports to scan, separated by commas. Port ranges are separated by a hyphen between the minimum port and maximum port.

TCP Ports: Save

UDP Ports: Save

NOTE: Ports will be scanned once per day.

Endpoint Analyzer Report

Jump Item Type ▼

Jumpoint ▼

Include open ports that were already marked as expected.

Show Report
Download Report ▼
Reset

Jumpoint Management

Better manage your installed Jumpoints. Jumpoint information on /login now includes the host system's public and private IP addresses, hostname, and comments. Easily redeploy a Jumpoint to a new host, with the new Jumpoint replacing the old one for any existing Jump shortcuts associated with it. Jumpoints can be clustered to provide redundancy and additional load capacity for critical network segments. Additionally, Jumpoints no longer require a user to be assigned to them directly.

Jumpoint Management

Add New Jumpoint

Jumpoints	
kgaipal_w10_esx64 (kgaipal_w10_esx64) - Not Installed Clustered Jumpoint with 0 node(s). kgaipal_w10_esx64	Edit Delete Add Node ▼
Remote Operations (operations) - Online since December 8 2015 03:06:40 PM UTC Clustered Jumpoint with 2 node(s). Shell Jump is disabled. Use for accessing X25 systems	Edit Delete Add Node ▼
JXNPLWS03605 - Online since December 8 2015 03:06:40 PM UTC Public IP is 172.19.250.155. Private IP is 172.19.250.155.	Delete
JXNPLWS03626 - Offline since December 3 2015 09:36:01 PM UTC Public IP is 172.16.0.150. Private IP is 172.16.0.150.	Delete
Server Maintenance (maintenance) - Offline since December 3 2015 11:15:59 PM UTC Standalone Jumpoint on host WIN-I80FDL2C9ID. Public IP is 172.16.0.150. Private IP is 192.168.152.128. Use for maintenance on the Omega servers.	Edit Delete Redeploy

▼ ↑ **Jumpoint Configuration Help**

From here you can administrate Jumpoints. A Jumpoint allows a user to upload the Bomgar PAM Endpoint Client to machines on remote networks. The networks a Jumpoint provides access to are collectively called a Jump Zone.

NOTE: Users will receive a prompt and still need authorization credentials on the endpoint that they are attempting to Jump to before the operation will succeed.

NOTE: The "Redeploy" option allows a user to uninstall the existing Jumpoint and download a new installer that will take its place.

To set up a Jumpoint:

1. Log into this website and click the "Add New Jumpoint" button.
2. Describe the Jump Zone in the name field, and give permission to users or groups who should be able to utilize that Jumpoint.
3. Click the "Add Jumpoint" button to add the new Jumpoint.
4. Use the "Download" link to download the Jumpoint installer. If you are currently at the machine on which the Jumpoint is intended to run, run the installer now. However, you may wish to send the downloaded installer to someone else who will install the software on some other machine. The installer is valid only for 7 days after it is downloaded.
5. While the Jumpoint is being installed the user will have the opportunity to set a date/time for the Jumpoint to activate itself and to set a date/time for the Jumpoint to uninstall itself.
6. After the Jumpoint is installed and active a user that has been granted access can log in and will see the Jumpoint in a list. He or she will be able to upload the Bomgar PAM Endpoint Client to endpoints in the Jump Zone to which the Jumpoint provides access or initiate RDP/SSH sessions to endpoints within the Jump Zone.

To set up a Jumpoint Cluster:

1. Log into this website and click the "Add New Jumpoint" button.
2. Describe the Jump Zone in the "Name" field, and give permission to users or groups who should be able to utilize that Jumpoint Cluster.
3. Click the "Add Jumpoint" button to add the new Jumpoint.
4. Use the "Add Node" link to download the Jumpoint installer. If you are currently at the machine on which the Jumpoint is intended to run, run the installer now. However, you may wish to send the downloaded installer to someone else who will install the software on some other machine. The installer is valid only for 7 days after it is downloaded.
5. After one or more Jumpoint nodes are installed and active a user that has been granted access can log in and will see the Jumpoint in a list. He or she will be able to upload the Bomgar PAM Endpoint Client to endpoints in the Jump Zone to which the Jumpoint provides access or initiate RDP/SSH sessions to endpoints within the Jump Zone.

When selecting a system to host a Jumpoint, keep the following criteria in mind:

- The host system should be a system on the same local area network as the systems to which you wish to Jump.
- The host system should be a system with high availability.
- **IMPORTANT:** The host system should NOT be a system already being used as a server. File servers, print servers, web server, email servers, etc. all make poor choices for Jumpoint host systems. Jumpoints attempt to close any active network connections to the target system before attempting the Jump, for security purposes. A Jumpoint that coexists on such a server will often report "Network error disconnecting from host" messages when attempting to Jump, as it attempts to close a network connection but fails to do so because some other software is actively using that network connection.

Mass Import of Endpoints

When creating a large number of Jump shortcuts, you can import them via a spreadsheet in the /login interface or via the API. Importing Jump Items saves time and effort over manually adding each one in the access console.

Jump Shortcuts Mass Import Wizard

Download a Template suitable for importing Jump Shortcuts:

Upload Jump Shortcuts Mass Import Template

Session Forensics

Command shell recordings are now included in Session Forensics searches. Successful matches in stored shell recordings automatically take the user to that point in time in the recording.

Access Session Forensics Results					
Back to Reporting					
Filter:					
• Events matching the search phrase "ipconfig"					
Time	Endpoint	Event	Text Match	Recording	Details
2015-11-20 21:50:56 UTC	JXNPLWS03605	Remote Shell Event	ipconfig	View	Details

Updates for Users

Bomgar Privileged Access Management 15.3 contains the following updates for Bomgar users.

Feature
Bomgar Privileged Web Gain secure access to endpoints through a web-based access console. The web access console removes the requirement of having to download and install the Bomgar access console client, enabling quicker access from more locations.
Change Management Workflow Bomgar access requests can now require a Ticket ID to be entered as part of the access request process. Once entered, the request is sent to your change management system, where it can be programmatically denied or allowed using the Bomgar API.
Linux Service Mode Jump Client The Linux Jump Client has been modified to allow installation as a service. During installation, the service creates its own user account to monitor active sessions on the endpoint. A service mode Jump Client allows for capabilities such as reboot and auto-reconnect, running applications as an admin, and Jumping to the endpoint even if no user account is currently logged in.
Mobile Access Console Enhancements From your iOS or Android mobile access console, use Remote Jump shortcuts and Remote Desktop Protocol shortcuts to securely connect to endpoints. Additionally, from your mobile access console, access Jump Items which have in place a Jump Policy requiring external authorization. Specify a message and a timeframe for future access. Once access is approved, you can access the Jump Item during the authorized time frame.
Multifactor Authentication Implement native multifactor authentication using a secure second factor access code emailed to a user. After the local user enters their username and password in either the access console or /login, they receive an email with a secure access code which they must enter before login succeeds.

Bomgar Privileged Web

Gain secure access to endpoints through a web-based access console. The web access console removes the requirement of having to download and install the Bomgar access console client, enabling quicker access from more locations.

Bomgar Access Console

Web Access Console

[Launch Web Access Console](#)

Desktop Access Console

Choose Platform Windows® (x64)

[Download Bomgar Access Console](#)

Follow these steps for initial login to the Bomgar Access Console:

1. Download and run the Bomgar Access Console software.
2. Follow the installation wizard to install the software.
3. When the installation is complete, run the Bomgar Access Console and enter your Username and Password at the login prompt.

B Q Access Console

All Jump Items

Personal

Team: Remote Access

Team: Server Issues

[REFRESH ALL](#)

Frequently Used Jump Items

All Jump Items

Name ▲	Method	Group	Status	Last accessed	
IE11WIN7	Jump Client	Server Issues	Passive [Unknown]	Never	
judges	Shell Jump	Remote Access	Available	11/20/2015 3:57 PM	
JXNPLWS01735	Jump Client	Server Issues	Active [Online]	11/20/2015 3:51 PM	
JXNPLWS03600	Local Jump	Remote Access	Unavailable	Never	
JXNPLWS03927	Remote Jump	Remote Access	Available	11/17/2015 4:08 PM	
JXNPLWS08204	RDP	Remote Access	Available	11/10/2015 8:59 AM	

Change Management Workflow

Bomgar access requests can now require a Ticket ID to be entered as part of the access request process. Once entered, the request is sent to your change management system, where it can be programmatically denied or allowed using the Bomgar API.

Jump Policies :: Ticket System

Ticket System URL

Upload a certificate for HTTPS connections

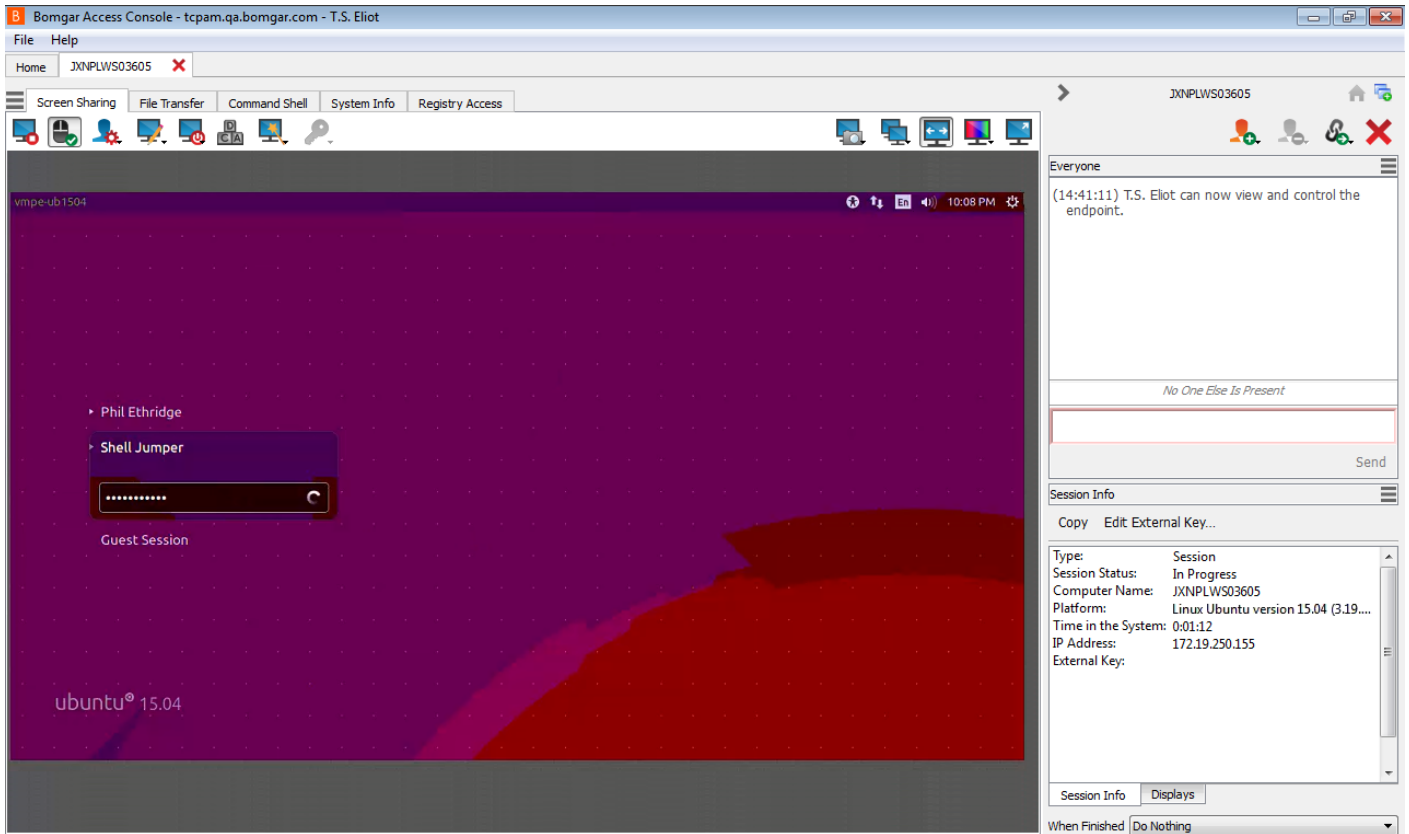
Certificates must be in PEM or DER format. No certificate has been uploaded. The appliance's built-in certificate store will be used to establish trust.

Ignore SSL certificate errors
NOTE: This could potentially make you vulnerable to SSL man-in-the-middle attacks.

User Prompt

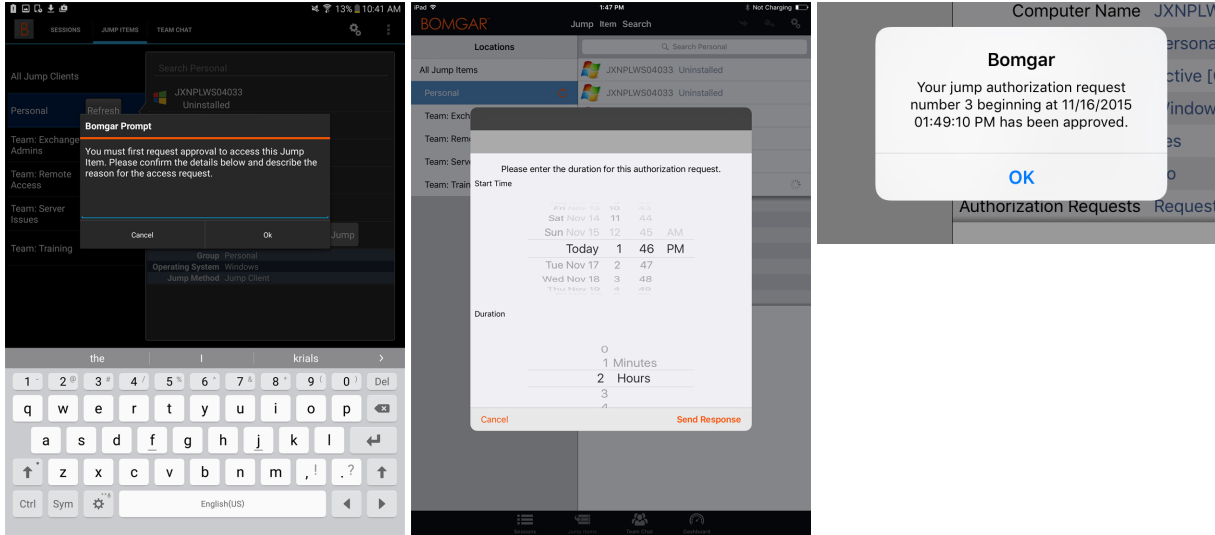
Linux Service Mode Jump Client

The Linux Jump Client has been modified to allow installation as a service. During installation, the service creates its own user account to monitor active sessions on the endpoint. A service mode Jump Client allows for capabilities such as reboot and auto-reconnect, running applications as an admin, and Jumping to the endpoint even if no user account is currently logged in.



Mobile Access Console Enhancements

From your iOS or Android mobile access console, use Remote Jump shortcuts and Remote Desktop Protocol shortcuts to securely connect to endpoints. Additionally, from your mobile access console, access Jump Items which have in place a Jump Policy requiring external authorization. Specify a message and a timeframe for future access. Once access is approved, you can access the Jump Item during the authorized time frame.



Multifactor Authentication

Implement native multifactor authentication using a secure second factor access code emailed to a user. After the local user enters their username and password in either the access console or /login, they receive an email with a secure access code which they must enter before login succeeds.

Login

Username rfrost

Enter the emailed login code

Send