BOMGAR™

What's New in Bomgar Privileged Access Management 15.3

TC:12/21/2015

Table of Contents

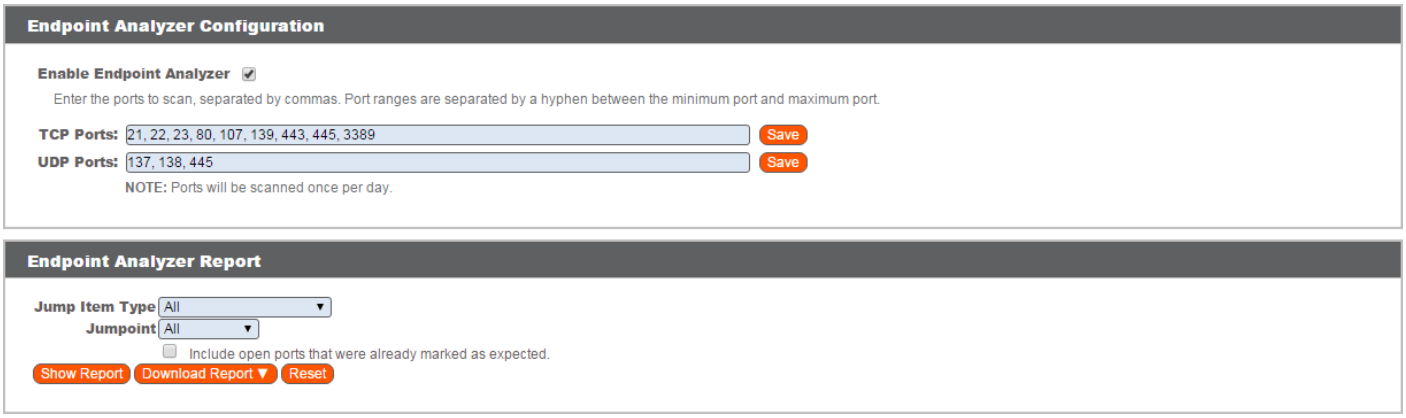
Updates for Administrators

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.

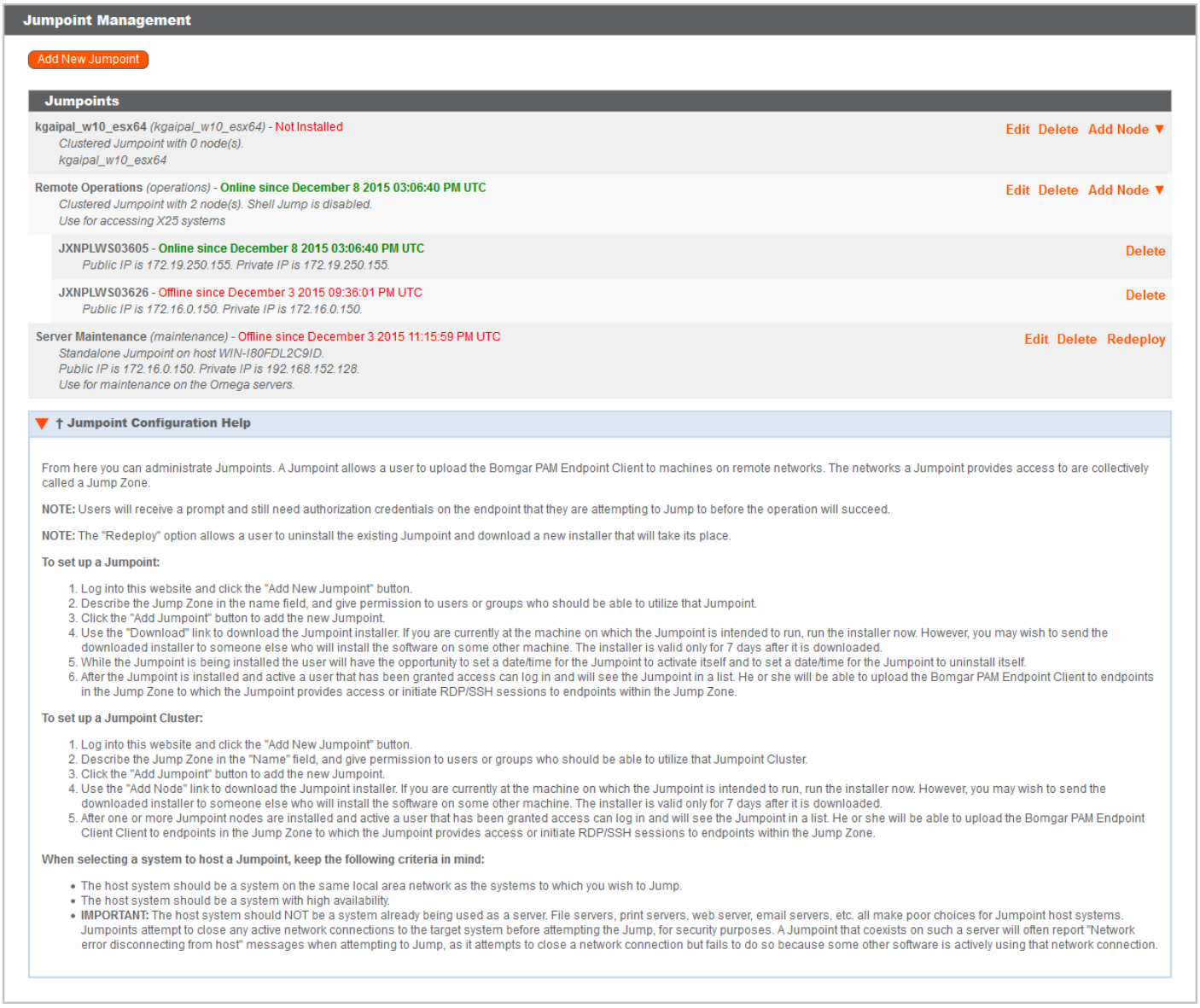
Endpoint Surface Analyzer

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.



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.

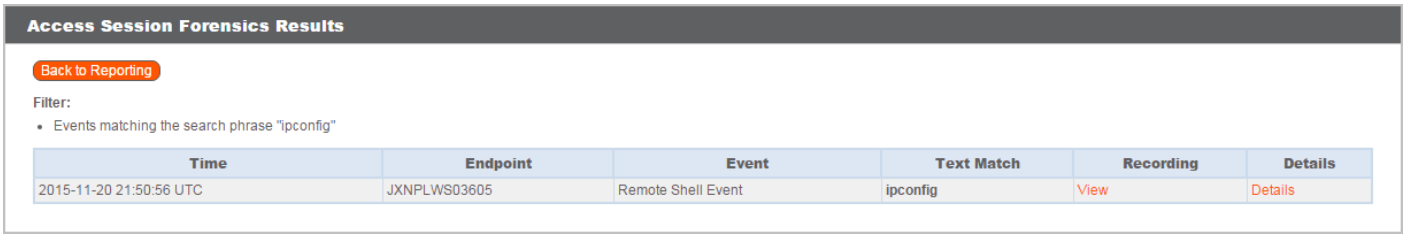


Mass Import of Endpoints

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.



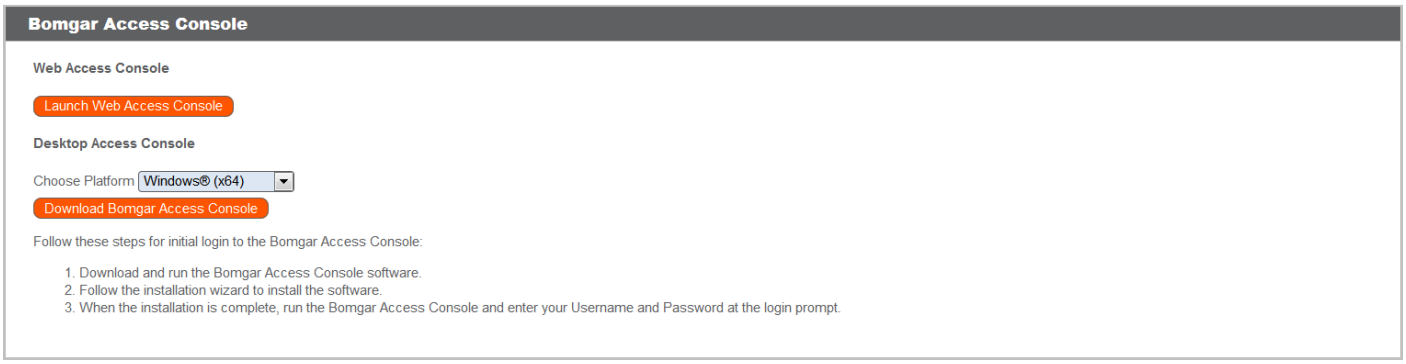
Updates for Users

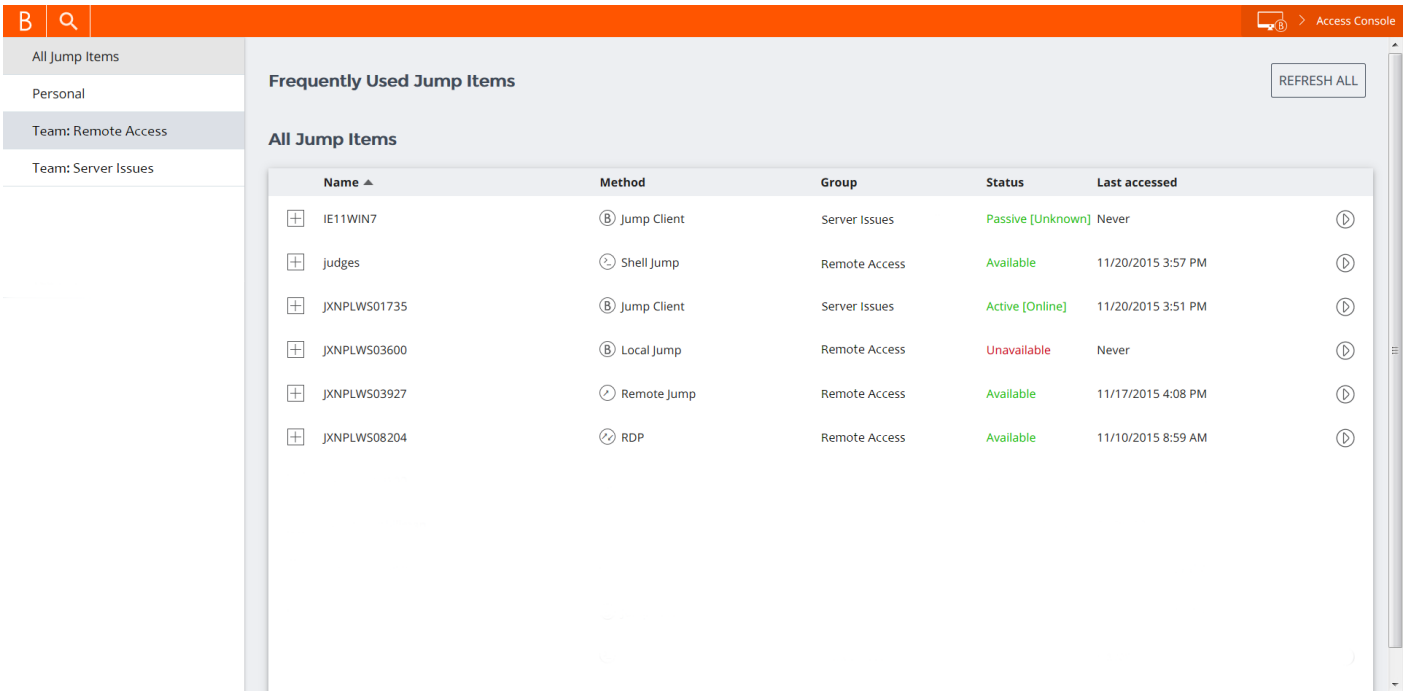
Bomgar Privileged Access Management 15.3 contains the following updates for Bomgar users.

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

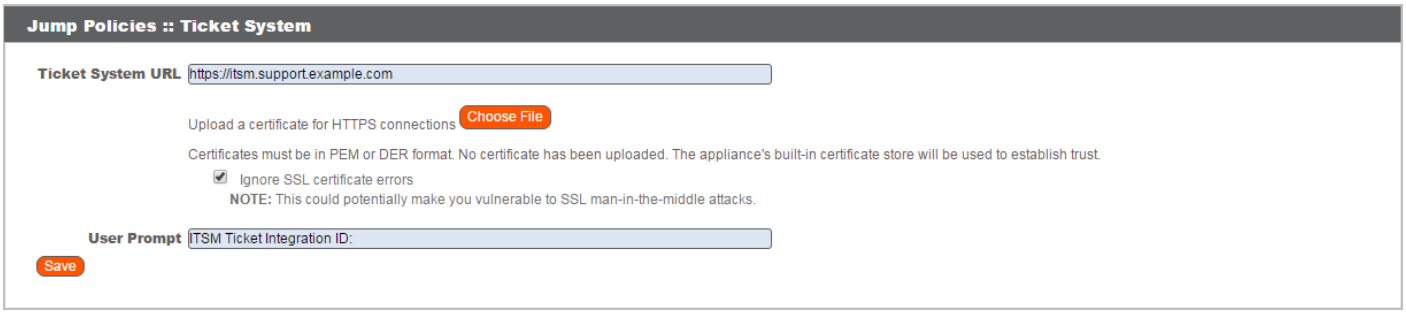
Gain secure access to endpoints through a web-based access console. The web access console removes the requirement of having to download and install the Bomgar access console client, enabling quicker access from more locations.





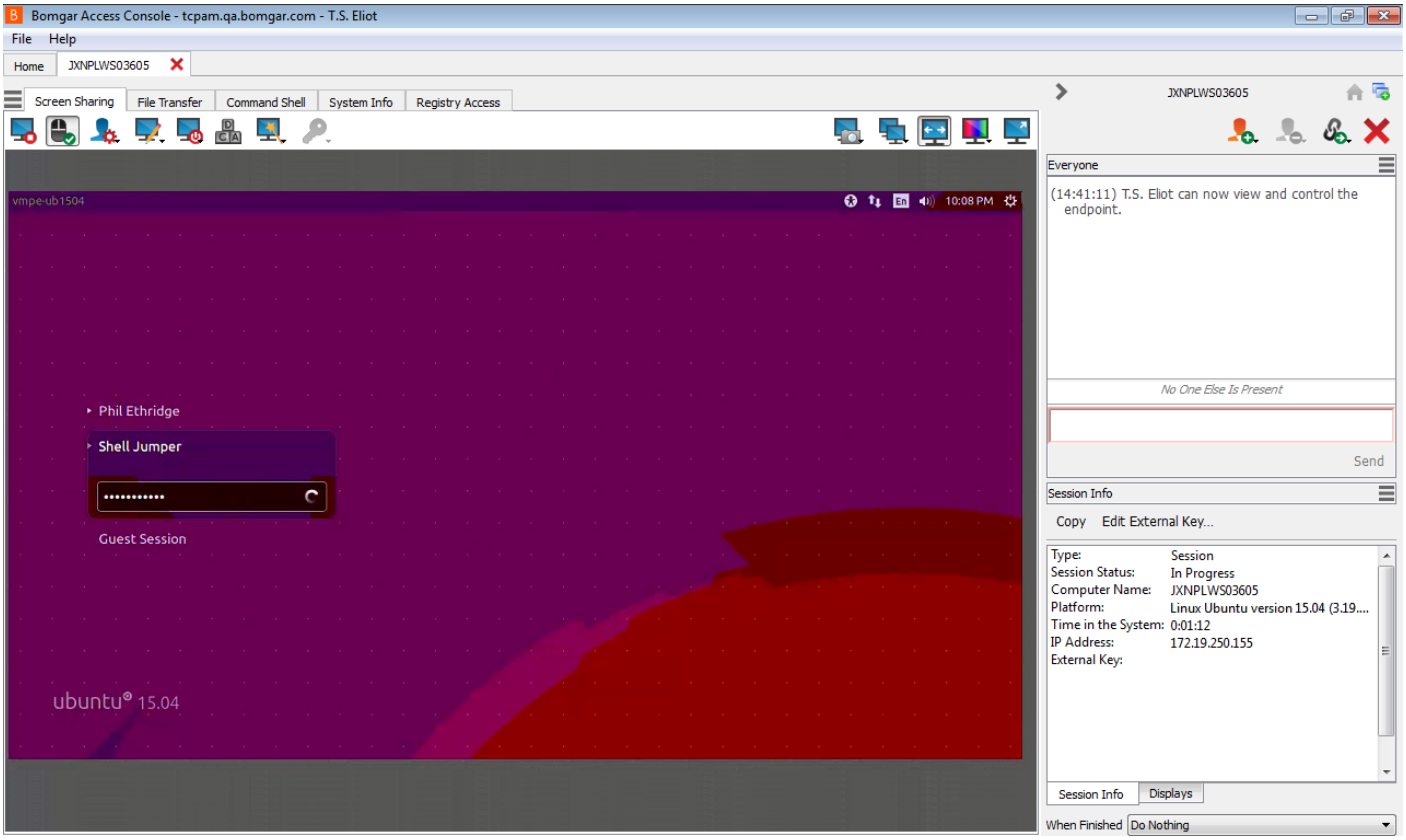
Change Management Workflow

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.



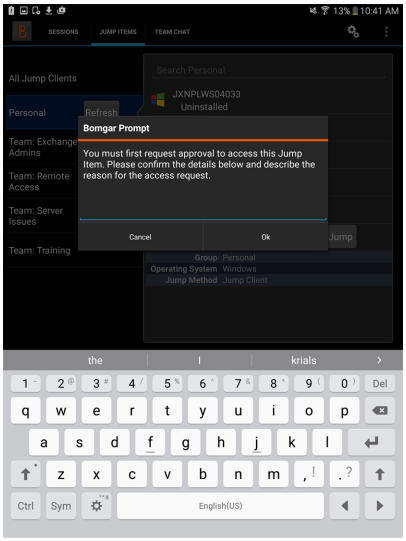
Linux Service Mode Jump Client

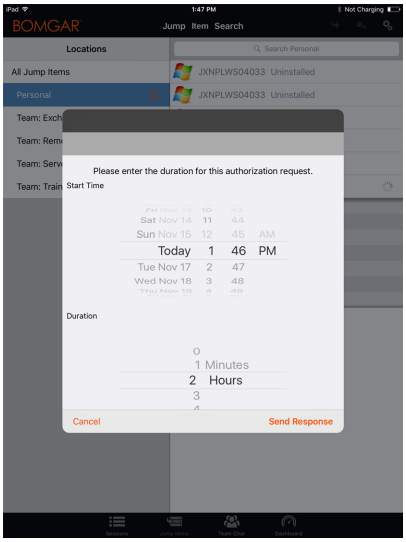
The Linux Jump Client has been modified to allow installation as a service. During installation, the service creates its own user account to monitor active sessions on the endpoint. A service mode Jump Client allows for capabilities such as reboot and auto-reconnect, running applications as an admin,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

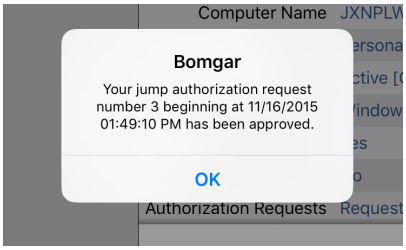


Mobile Access Console Enhancements

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.