

Remote Support for Locked-Down Networks

Remote support can be a great time-saver when accessing remote desktops over the LAN/WAN or supporting remote customers over the internet. But how do you access a remote, locked-down network to support systems that are not connected to the internet?

Typically, locked-down networks can only be supported by local technicians. But this creates problems for the support organization. Locked-down networks require onsite visits which delay incident resolution and raise costs.

In addition, local technicians still use remote support tools, but most LAN-based remote support tools [VNC, RDP] lack the audit logging or access control required for security. This undermines the reason the network was locked-down in the first place -- to ensure security!

How can your support organization

- Support locked-down networks without going on site?
- Use remote support without compromising security?

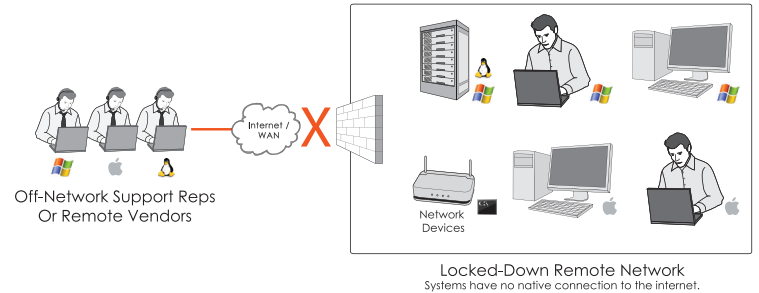


Fig. 1: Locked-down networks require local technicians for support, which can compromise security.

Bomgar's Solution: Jump Zone Proxy

Jump Zone Proxy enables off-site support technicians to connect to systems on remote, locked-down networks. It does this by using a Bomgar Jumpoint - a node installed on a remote network - to proxy connections for clients on the network that do not have a native internet connection, allowing traffic only to the Bomgar appliance.

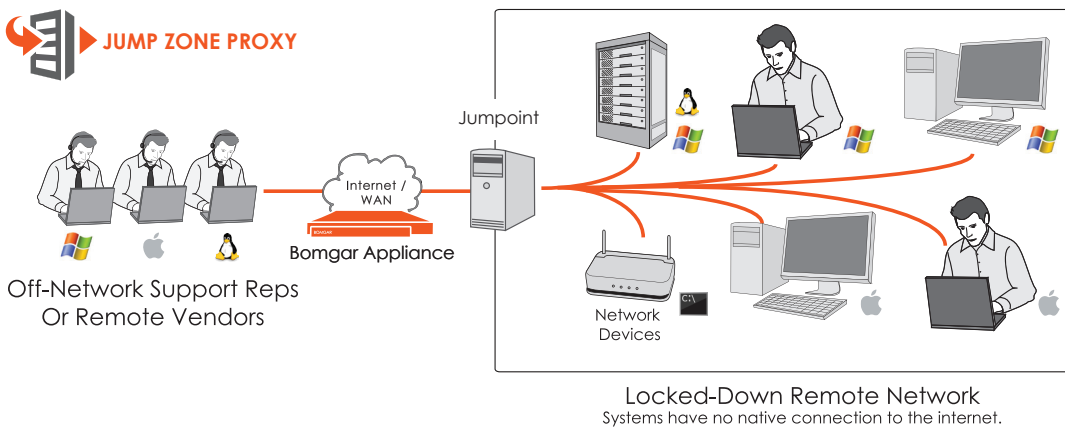


Fig. 2: Jump Zone Proxy routes all outbound traffic through the Bomgar appliance, enabling off-site support technicians to control locked-down systems securely over the internet.

Secure Remote Access

Administrators can enable Jump Zone Proxy whenever they install or configure Jumpoints.

Managers can use a simple Bomgar wizard to define which ports the Jump Zone Proxy uses and which IP ranges can access it.

Once enabled, managers can report on and view videos of support sessions performed through Jump Zone Proxies.

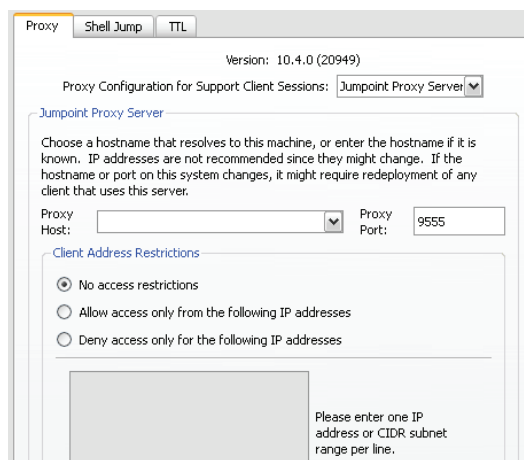


Fig. 3: Administrators can enter the DNS or IP address to use as the listening interface, set which port to use, and define the IP ranges that can connect through the Jump Zone Proxy.

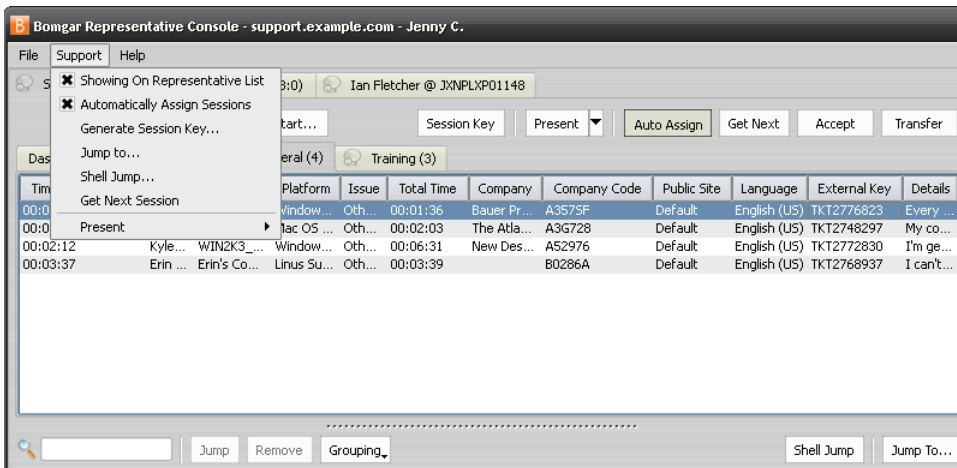


Fig. 4: Jump Zone Proxy requires technicians to use the Bomgar Representative Console, ensuring access control measures and audit requirements apply to support sessions that involve remote, locked-down networks.

Additional Security Measures

In addition to enabling integrated access control and a detailed audit record, Jump Zone Proxy includes additional security parameters.

Administrators can determine which support technicians or groups can use Jump Technology, and which remote networks they can access. They can set expiration dates on Jumpoints, too. Ultimately, technicians can only access remote systems if they know the login credentials on the individual systems themselves. Jump Zone Proxy satisfies the needs of the most security-conscious organizations without making remote access a cumbersome and costly ordeal.

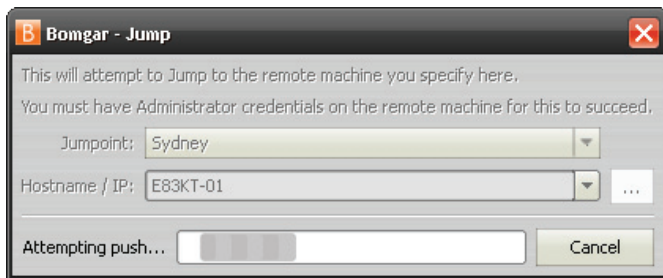


Fig. 5: Technicians with permission to use Jump Technology can see the networks they have permission to access in the Bomgar Representative Console.

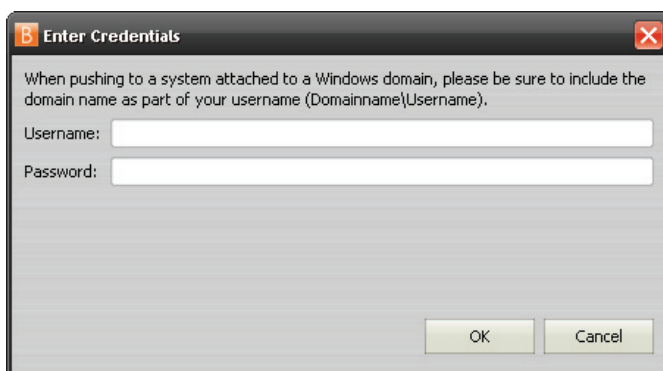


Fig. 6: Technicians must know the login credentials on the remote computers they wish to access.

Integrated Access Control

When technicians use legacy remote control tools or go onsite for support, your support organization risks compromising data security and loses visibility into the support process.

With Jump Zone Proxy, support technicians access locked-down systems in remote networks by *Jumping* to them from the Bomgar Representative Console.

Because Bomgar integrates with identity management protocols, such as LDAP and Active Directory, the centralized access control used for all remote support sessions also applies to those that take place on remote locked-down networks.

Centralized Audit Record

Using Bomgar to support systems on remote, locked-down networks also has implications for your audit trail.

Not only does Bomgar require every support session to pass through multiple layers of stringent security, it creates a detailed record of every session, too, including annotated videos.

If systems in a remote network have been locked down to increase security, there's no more secure way to support them than with Bomgar.