



The Problem of Not Integrating Remote Support

Many legacy remote control tools let a rep remote into a user's system without a single log of the connection. However, in today's regulated business environment, your enterprise is taking a big risk if remote support is not integrated with your existing identity management.

Integrating remote support with your internal directory ensures you can account for who is doing what during support sessions. Bomgar also enables granular control over support representative permissions through individual or group policies defined in your own directory.

Bomgar's Solution: Identity Management Integrations

Bomgar's integrations with many industry-standard security providers enable you to manage your technicians' accounts through your existing account directory. If your directory server is located behind a different firewall than the Bomgar appliance, you can configure the firewall to enable the transmission of information or you can use a connection agent to enable secure communication without changing firewall configuration.

Bomgar's identity management integrations include:

- **Integrate with LDAP and AD**
- **RADIUS for multi-factor authentication**
- **Kerberos for single sign on**

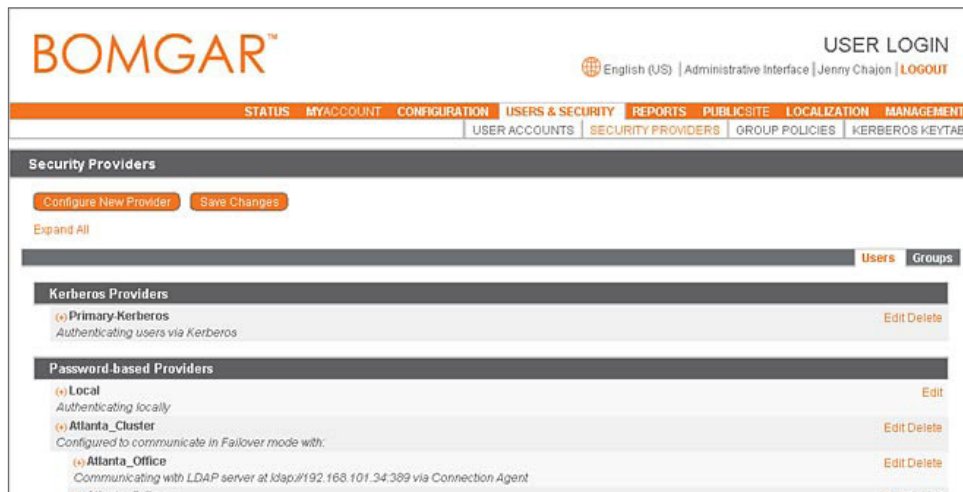


Fig. 1: Bomgar integrates with many industry-standard security providers so you can manage your technicians' accounts through your existing account directory.

Use Your Existing User Database to Create Bomgar Accounts

Instead of creating an account for each support representative in the Bomgar administrative interface, you can configure Bomgar to authenticate users directly from company directories. Using the pre-existing hierarchy and group settings already specified in these directories, you can assign account settings to user groups rather than assigning privileges manually to each user.



Consistent Authentication

By integrating Bomgar with your existing directory, users can log in using their existing authentication credentials. This eliminates a lot of work for the administrator and your technicians don't have to remember another username and password.

Automatic Status Updates

Bomgar can read accounts straight from the directory. Because of this, any change in a user's status will automatically update in Bomgar's user settings and privileges. No configuration is required. For example, if someone moves from the internal support group to the customer support group in the company directory, Bomgar will read that user as a member of the customer support group and assign privileges for that group automatically.

Automatic Deletion

If a support representative moves to another area that does not use Bomgar or leaves the company, the user's privileges are automatically removed from Bomgar when he or she is deleted from the company directory. The user account information only appears in Bomgar for reporting purposes.

Why Identity Integration Is Important

The 2009 Data Breach Investigations Report from the Verizon Business RISK Team reports that in "approximately four out of 10 hacking-related breaches, the attacker gained unauthorized access to the victim via one of the many types of remote access and management software."

With this risk, it's important that your remote support solution give you a clear audit trail of who access what systems inside and outside your network. Bomgar simplifies this with identity management integrations.

Gartner's PC Remote Control Security: Risk and Recommendations report reaffirms the need to use your internal directories to authenticate users:

"This is another compelling reason to use strong user authentication and to bring administration and remote control directory services in-house. If external services must be used, then seek assurances and assignment of liability from external service providers."

(PC Remote Control Security: Risks and Recommendations Gartner, April 2009)