Polaris Support Remote Access

Polaris has recently implemented a remote support access solution with SecureLink® that will make remote support access more secure and efficient for all Polaris customers, and will help customers who are pursuing PCI-DSS compliance requirements for e-commerce.

> **Note:**
> While it is Polaris Library Systems' responsibility to ensure that the Polaris ILS application meets the standards of the PCI Security Standards Council, it is the library's responsibility to make sure its network structure, network maintenance, policies and procedures meet these standards. Among these policies and procedures are remote access practices.

Polaris support personnel will no longer directly connect to library servers using Remote Desktop and server account credentials stored at Polaris. Instead, customers with PCI-DSS Compliance requirements manually control all Polaris remote support access to library servers. The two-factor authentication requirement is met as follows:

- Polaris Support staff must first log into the SecureLink remote access service using their PCI-compliant Polaris username and password (non-shared, complex, etc.).
- Using SecureLink Quick Connect, a one-time access token required to complete the connection will be generated.
- The library will receive the token either via e-mail or verbally and, to enable the connection, must enter that token within 15 minutes on the server to which they intend to provide remote access.

Polaris staff will not know or have access to the customer's server passwords and will not have unattended access to customer servers. SecureLink provides a session logging function and remote access is disabled after the connection is closed. Any further connections will require that this authentication process be repeated.

Customers without PCI-DSS compliance requirements can use SecureLink GateKeeper to maintain server passwords and manage Polaris remote support access rules. With both the GateKeeper and Quick Connect solutions, Polaris will not know or have access to the customer's server passwords, and the customer will have complete control of remote access to their servers.

Contact your Polaris Site Manager for further information about implementing SecureLink.

Important Notes About PCI-DSS Compliance

- Polaris is confident that our use of SecureLink Quick Connect for remote support access will help our customers comply with PCI-DSS requirements, but only with respect to Polaris's remote support access. Each customer must abide by the PCI-DSS compliance determinations made by the auditing QSA (Qualified Security Assessor) and/or Acquirer with whom the customer contracts for e-commerce; this agent has the final authority.
- Many PCI-DSS requirements are based on non-Polaris components such as the customer's security policies and management of their local network, firewall, users and passwords. The PCI rules specific to remote support access do not pertain only to Polaris and will apply to any third-party vendors that may require access to library servers, which may include Microsoft, Dell, or others.
- Polaris ILS software is PA-DSS compliant and is one component in a fully integrated PCI-DSS compliant e-commerce solution. To meet PCI-DSS requirements not related to the Polaris software, the library must comply with a list of PCI-mandated network and security policies. If achieving PCI-DSS compliance in a fully integrated environment is beyond a library's capacity, Polaris offers an e-commerce solution through a partnership with Comprise Technology, Inc., that reduces the PCI scope using network segmentation, and typically has a much lower PCI-DSS compliance threshold. The Comprise SmartPAYpayment solution is suitable for both Polaris Virtual Private Cloud (Hosted) and Polaris ILS turnkey customers. For more information, contact Polaris Customer Sales at 1-800-272-3414.