

## ***CrossTec Remote Control - Optimizing Security and Efficiency***

### **Introduction**

Remote Control security largely depends on the configuration and implementation of any product that is being used, not necessarily on a subset of available features that are usually disabled by default. All remote control programs must be able to be locked down with features like strong authentication, logging, encryption, user acknowledgements, and configuration passwords before deployment to maximize security. It is also important that a remote control program stay simple; there should be no need for dedicated hardware, expensive or complex licensing and poor technical support, after all it is meant to maximize your IT staff's efficiency, not create added overhead. Most organizations centralize authentication and overall Windows security using Windows Active Directory (AD) and Group Policy, so the deeper a remote control program can integrate into AD, for authentication, logging, and deployment, the more powerful and flexible a tool it becomes. CrossTec Remote Control (CRC) meets and exceeds all of these security requirements to allow an organization of any size to securely deploy remote control software with minimal overhead and maximum security.

### **Optimizing Security and Efficiency**

By means of its design, CRC uses Active Directory Users and Security Groups or Users for authentication, and allows Clients to be deployed and updated via Group Policy Objects, eliminating the need for a centralized, remote control authentication server. The CRC Client does not communicate with an additional server to authenticate or log, instead the Clients authenticate directly with the Domain Controllers in true AD fashion and either log to the Windows Event Log or a flat file on the network that can be protected and appended to. This design eliminates additional authentication traffic, complicated Client LDAP configurations and the requirement of a dedicated server with a backend database. Authorization is a function of authentication in AD of Windows Users and Groups. If you have AD, then you already have centralized authentication and authorization, regardless of the remote control program you buy, to the extent that the program integrates into your current AD scheme. The redundant authentication points in AD are called Domain Controllers, by licensing and maintaining an additional server product on your network, that uses a backend database, instead of securing your network, you are actually adding IT overhead and costs. If you use CRC, then it'll quickly be apparent that implementing a stand-alone, third party server, which requires constant maintenance and expertise to handle, in addition to your AD Domain Controllers, is an unnecessary and expensive step, that achieves the same purpose - role-based authentication for remote control users via Windows groups.

### **The Bottom Line**

With support for cutting-edge features such as 64bit OS support, real-time Client thumbnail monitoring, enhanced graphics support (OpenGL, multi-monitor), deploying Client configurations via Active Directory GPOs, impersonating the Windows logged on user during functions such as file transfer, etc... CrossTec feels it has created a remote control program that is truly flexible enough to meet most of today's demanding network infrastructures while keeping it simple!

### **NetOp Security Server Requirements**

NetOp adds a remote control specific Authentication server on top of your regular Active Directory authentication scheme and centrally logs to this server called the NetOp Security Server. Putting all the logs into a backend SQL database in a format that is unique to NetOp and adding an unnecessary layer of authentication presents a problem where an issue with the Security Server or with the backend database can mean loss of event logs or worse, not being able to remote control any machine at all because of the inability to authenticate. NetOp logs also require NetOp expertise to read and understand, with CRC you can log to a central file if you wish, or the Windows Event Log which can be retrieved using Microsoft tools or a third-party Windows event logging solution you may already have. CRC logs are easy to understand and extremely detailed, with information like Windows Logon Name in the event by default, without requiring customizations. For more information on CRC logging please see the CRC User's Manual, and for more information about centralizing ALL of your important Windows Event Logs please check out the CrossTec SIEM tool Activeworx Security Center [www.CrossTecSecurity.com](http://www.CrossTecSecurity.com)