CRS Notify Technical FAQ

What is it?

CRS Notify is an internet-based panic button program consisting of two components – a client and a local server. Any number of clients can connect to a local server, which then connects to the centralized CRS authentication server. When an alert is raised, phone calls, text messages and emails go out to designated responders, and an alert window appears on each machine that is running the CRS Notify client software. This alert window can be used to add observations and updates to the active alert situation or to monitor the situation in real-time as it unfolds.

Do I have to install the client and server on every computer on the network?

No. Typical installations will only have one server per network, and the clients only need to be installed on computers that will either be used as panic buttons or computers that need to be notified during an active alert situation. The client and server can run on the same machine if necessary, but we recommend running the server on a separate machine that is always online. Some computers may not need the client at all – in situations where people may only need to receive information about an event, those people could be added as email or text message recipients. They would still receive information about an event as it unfolds but they would not be able to add comments to the alert event.

I have multiple sites connected by a WAN or VPN, can CRS Notify work in that environment?

If you have multiple physical locations, it is best to set up a local server at each location and connect those locations through the CRS Dashboard. The phone calls, text messages and emails that go out as a part of an alert event all contain location-specific information, which could be confusing or delay the time it takes to receive assistance if the physical location that raised the alert isn't the same as the location where the WAN or VPN originates.

What impact will this have on my network?

We designed CRS Notify to have a minimal impact on local resources, both in terms of storage space and network traffic. The client takes up less than 4MB on disk and the server is small enough to fit on an old 3.5" floppy disk at less than 1MB. The clients send small heartbeat messages out to the server consisting of a few bytes each and the server sends similar heartbeat messages out to the central authentication server.

What type of information is transmitted? Is it secure?

Until an alert has been raised, only heartbeat, authentication and configuration information is transmitted. After an alert has been raised, clients send encrypted alert description information to the local server. The local server passes this information to the CRS authentication server, which sends the phone calls, text messages and emails, and transmits the information to any remote connected servers (your corporate office, for instance, or possibly a location across town). The information is also returned to the originating server to confirm that the notifications were sent to the appropriate responders. The alert information is encrypted using an AES-256 encryption algorithm.

When a location is not in an active alert state, configuration changes made on the CRS Dashboard are pushed to the appropriate local servers. For instance, changing a user's information (such as password, room assignment or phone number) on the CRS Dashboard initiates a push of the updated information to that user's location. The new information is saved to the local server and will be active the next time the user logs in.

If I have the client deployed to several computers, am I going to have to update each one when a new version is released?

Recent versions (1.8 and newer) of the CRS Notify client automatically update to the latest version when the program starts. This process is set to update by default in case a user has stepped away from their keyboard when the update screen appears.