



## Connectivity White Paper

June 2, 2010

Critical Reach (aka TRAK) is used to create and distribute photo bulletins to other Critical Reach (CR) desktops/laptops, and to email addresses and to fax machines.

There are two central servers involved in the operation of the Critical Reach system. The **mail server** holds bulletins for retrieval by the CR desktops. The **web server** handles database operations and is the submission point for bulletins being transmitted from CR desktops.

When a CR desktop transmits a bulletin, it sends the bulletin to the web server. The web server builds a distribution list and sends the bulletin to the mail server for retrieval by CR desktops, and for distribution to email and fax destinations.

### CR Mail Server

The DNS name for the mail server is *trak-2.smrn.com*. Its IP address is 204.152.189.72. CR desktops connect to this server using authenticated POP3 protocol via port 110. The CR system handles email sessions via internal code, without use of a commercial email client on the desktop. All connection sessions are initiated by the desktop outbound to the server. The server never initiates contact with the desktop. See page 2 for connectivity test procedures.

Each CR desktop polls its authenticated POP3 account on the mail server every two minutes. When a CR desktop finds a waiting bulletin in its POP3 account, it retrieves the bulletin as an email attachment. The CR desktop then processes/validates the retrieved bulletin and puts it into the CR desktop application's *InBox* on the Main Menu. The *InBox* then alerts the user, via screen blinks and audio beeps, that a bulletin has been retrieved. Bulletins retrieved from the mail server are processed strictly as data by the CR desktop software. The system automatically discards any email retrieval that is not a valid CR bulletin.

If there is a firewall between the CR desktop and the CR mail server, it must allow POP3 retrieval from the CR desktop to IP address 204.152.189.72 on port 110. If the firewall requires authentication, it must be provided through some mechanism external to the CR desktop software.

### CR Web Server

The DNS name for the web server is *trak-1.smrn.com*, and its IP address is 204.152.189.71. CR desktops connect to this server using HTTPS over SSL, via port 443. All connection sessions are initiated by the desktop outbound to the server. The server never initiates contact with the desktop. See page 2 for connectivity test procedures.

Each CR desktop periodically contacts the web server to keep its internal database up to date. It also contacts the web server to transmit a bulletin.

If there is a firewall between the CR desktop and the CR web server, it must be configured to allow HTTPS traffic outbound from the CR desktop to IP addresses 204.152.189.71 on port 443. If the firewall requires authentication, it must be provided through some mechanism external to the CR software.

If there is a Proxy Server involved, it is necessary to modify the CR desktop's INI file (CRConfig.ini shortcut on the desktop or c:/TRAK/TRAKClientConfig.ini), setting these four values in the [SOAP] section of the file:

```
ProxyServer=<name or IP address of the proxy server>
ProxyPort=<proxy server port number, traditionally 8080>
ProxyType=3
CheckHTTPStatus=No
```

Also, the Internet Explorer proxy settings should be configured appropriately (Tools/Internet Options/Connections/LAN Settings). This is tested by opening Internet Explorer, and accessing the URL <https://trak-1.smrn.com/trak/eab-le>. If **Internet Explorer** displays a dialog requesting a user id and password, then your proxy server is configured to require authentication. If you reach the CR address book login page, then authentication is not required and you can proceed.



## Testing Connectivity to the Two Servers

The list below shows the methods that can be used to test the connectivity from the CR desktop to the servers by using a Windows command window. A failure of the Ping test does not necessarily mean a lack of connectivity since the Ping protocol may be turned off by a network component somewhere between the desktop and the servers.

Test	Web Server	Mail Server	Successful Response
Ping	ping trak-1.smrn.com ping 204.152.189.71	ping trak-2.smrn.com ping 204.152.189.72	Test says it was successful
Telnet	telnet trak-1.smrn.com 443 telnet 204.152.189.71 443	telnet trak-2.smrn.com 110 telnet 204.152.189.72 110	< 443 shows a blank screen with a blinking cursor < 110 shows +ok welcome...
Browser	https://trak-1.smrn.com/trak/eab-le		EAB login page is shown

If none of the tests are successful, *tracert* is one possible way to determine where the connectivity is failing or is being stopped. However, since *tracert* depends on Ping, if Ping is blocked by a network component, this will also block *tracert*.

If the server DNS entries above cannot be successfully resolved, but there is connectivity to the IP addresses, then creating entries for *trak-1.smrn.com* and *trak-2.smrn.com* in the desktop's Windows HOSTS file should solve the problem.

## Reports for Connectivity Problems

The CR desktop software monitors the status of the connectivity between the desktop and the two servers. If a problem is detected, the user is alerted via a red dialog box on the desktop and a printed network connectivity diagnostic report is made available to assist IT personnel in correcting the problem.

## Notifications for Unviewed Bulletins

The CR desktop software constantly checks for any unviewed bulletins that have been received and notifies the user when new bulletins are available.

## Security

1. Only encrypted and authenticated access is allowed to the web server. The server is authenticated with a security certificate in addition to CR desktop UserID/Password.
2. Only the CR web server can send SMTP email to the CR mail server; no other entity can send email to it.
3. Access from the CR desktop to the mail server is strongly authenticated. When a CR desktop retrieves its bulletin on the mail server, it processes what it downloads as data, not as an exe or macro or script, etc.
4. There is no public access to the two CR servers.
5. Extra security can be implemented by assigning a static IP to the CR desktop and enforcing the source and destination IP addresses in a firewall policy. Or you can disable DNS and use a Windows Hosts file for DNS resolution for the two CR servers.

## Misc

1. The latest version of this document can always be downloaded from:  
<http://www.CriticalReach.org/Documents/Connectivity.pdf>
2. The 204 IP addresses and bandwidth referenced in this document are donated to Critical Reach. Thus, if you do a "whois" or other Internet information query on the addresses, you will find that the 204 addresses are donated by isc.org (the organization that operates the F root DNS servers around the world).