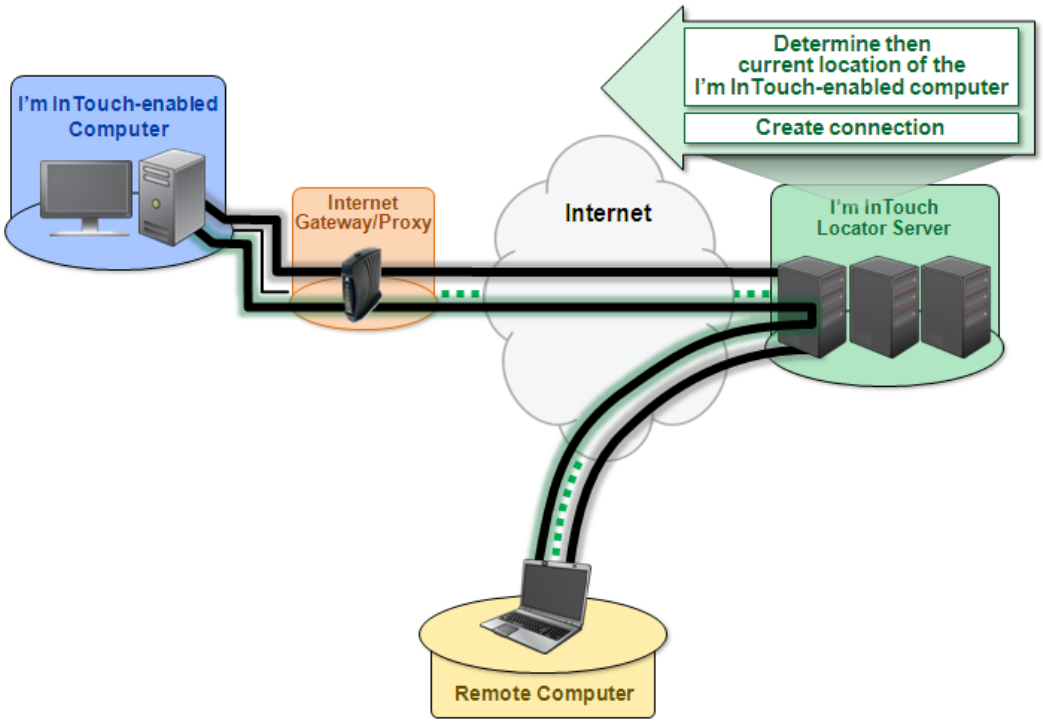
I’m InTouch Security Overview



I’m InTouch Architecture

I’m InTouch (US Patent #6928479, #6938076, #8234701) provides businesses or personal users a secure and cost-effective way to remotely access to their home or office computers. They can run programs, transfer files, manage email, contacts and calendar events, and do most thing they do while sitting at their computer.

Remote access is accomplished by installing the I’m InTouch enabling software onto the computer the user wishes to be able to access remotely. Thereafter the computer becomes I’m InTouch-enabled. The I’m InTouch patented technology (U.S. Patent Number #6928497, #6938076, #8234701) is managed by 01 Communique within a secure data center, locates the user’s I’m InTouch-enabled computer and connects it with the remote computer (accessing client), regardless of whether its IP address of the I’m InTouch-enabled computer is changing or static, behind firewall/router, or directly connected to the Internet.

The I’m InTouch-enabled computer maintains a SSL secure session with the I’m InTouch server by polling the server to see if any remote connection request has been made, using outbound HTTPS through port 443 on the firewall. As no port needs to be opened through the firewall (other than the usual Internet ports) you do not have to bypass or compromise your firewall and existing security policies of the business.

Encrypted Transport using Secure Sockets Layer (SSL)

Protection of the confidential business data is enforced by the utilization of the SSL HTTPS protocol. All traffic between the remote computer, server gateway, and the I'm InTouch-enabled computer, including screen images and file transfer are protected with the end-to-end SSL encryption.

Dual Authentication

The purpose of authentication is to ensure that the identities of the Locator Server, the Remote Computer and the I'm InTouch-enabled Computer are verified. I'm InTouch deploys a number of authentication processes to ensure that data exchange is permitted between trusted sources only.

During a remote session the Locator Server must first authenticate itself to the remote computer by supplying a digital certificate, issued by a trusted authority.

After knowing that the Locator Server is a trusted source, the user inputs the Computer Name (selected by the user during the installation of the I'm InTouch-enabling software) that can contain up to 64 characters of both letters and numbers. Long and complex Computer Names naturally provide stronger protection. The Locator Server checks to see if this is a valid Computer Name and that this workstation is currently on and running the I'm InTouch software, thereby being "registered" or polling with the Locator Server.

The Locator Server then passes a further authentication request to the I'm InTouch-enabled computer. Authentication is in the form of a login name and password that are stored only on the I'm InTouch-enabled computer and managed by its owner. The login name can contain up to 254 characters and the password can have up to 12 case-sensitive alphanumeric characters. This login name and password are encrypted and will not be seen on the server gateway.

Ongoing data exchange between the Remote Computer and the I'm InTouch-enabled Computer is encrypted and is managed through the Locator Server.

Security Features of the I'm InTouch Host Computer Program

To be remotely accessed, authorized computer must be I'm InTouch-enabled. After created an I'm InTouch account, the user will receive an activation email. Then use the computer that will become I'm InTouch-enabled to receive the activation email. Follow the simple instructions on the email to download and install the I'm InTouch enabling software. Installation requires physical access to the computer.

Authentication to the I'm InTouch-enabled computer requires a User Login Name and Password that are stored only at the I'm InTouch-enabled computer, eliminating the risk of passwords being stolen at the server gateway during an unlikely event of a system-wide hacker attack. Local management of the

authentication passwords at the I'm InTouch-enabled computers allows frequent user password updates by end-users which is a good security practice.

To help protect against dictionary attacks, I'm InTouch limits the number of times any user can attempt to login consecutively. By default, after three unsuccessful login attempts, access to the I'm InTouch-enabled computer is disabled for five minutes.

To minimize the risk associated with users leaving a remote session on a public computer without first logging out, inactivity time-outs are applied. After a user-defined time period of inactivity on the SSL session, the I'm InTouch-enabled computer will automatically terminate the session.

To provide assurance to the owner of the I'm InTouch-enabled computer that nobody can silently access his/her computer, a notice is displayed on the computer's screen whenever a remote computer establishes a connection to the I'm InTouch-enabled computer. In addition, users can always check the log to view the history of their last login. Both of these tools help to assure end-users that I'm InTouch is secure and safe to use.

Conclusion

In conclusion, I'm InTouch is an affordable and secure remote access solution that easily integrates into a users existing network and security architecture. It provides protective processes and the necessary tools to ensure that resources are always safe. These include thorough authentication of all devices and users involved in a remote session. All of these are delivered within a secure system architecture that does not require change to existing business network configurations. And most importantly all data exchange is safe, secure and encrypted.