

SECURED DATA COMMUNICATION

Support Automation service

Minimizes the likelihood of unauthorized access to an end-user's system



- ✓ Availability monitoring
- ✓ Remote control
- ✓ Support automation
- ✓ Intrusion protection
- ✓ Anti-virus management
- ✓ Patch management
- ✓ Asset management
- ✓ Software updates
- ✓ Specific problem alerts
- ✓ Resource monitoring
- ✓ Performance monitoring
- ✓ Registry management
- ✓ Service management
- ✓ Backup management
- ✓ Network discovery
- ✓ Windows event log tracking
- ✓ User access control
- ✓ User information management
- ✓ System maintenance
- ✓ Policy enforcement
- ✓ Software provisioning
- ✓ Software metering
- ✓ General system management
- ✓ General problem diagnosis
- ✓ General problem resolution
- ✓ Internal product maintenance

Best-of-the-breed Secured Data Communication

HandsFree Networks designed the Integrated Support Automation framework with comprehensive security throughout to deliver remote support solution that incorporated the most advanced security technologies. HandsFree Networks solutions are so ubiquitous on a network, and its main function is to resolve symptoms and execute system management and maintenance procedures, it is extremely protected from unauthorized use and infiltration. HandsFree networks multilevel security measures to ensure the absolute protection of customers and support representative data in every support session. Some of the many mechanism that we employ to safe guard your remote support session are:

SECURITY REGULATIONS AND COMPLIANCE

ReSOFT meets the privacy and security regulation for storage and transmission of data through state of the art security measures, including MD5 hashing of data such as DART configuration, DART execution and Event and data logging.

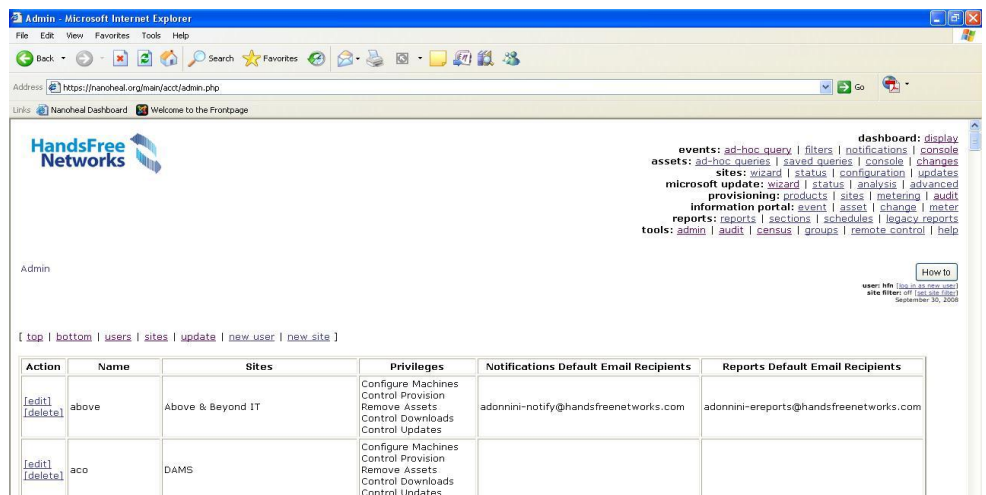
STATE OF ART SECURE COMMUNICATION

For maximum security, HandsFree Networks use encryption as well as industry standard protocol such as like SSL to ensure that your data is protected; this means that passwords are never stored anywhere and provides most secure way of accessing. Hashing is a one-way irreversible function while encryption is a two-way reversible thus provides maximum security function. All live session transactions, including text, image, desktop sharing and file transfer are completely secure.

ENSURE SAFE WEB ACCESS

Administrators access the HandsFree Networks server through a web interface after a secure logon process. For maximum web security, the HandsFree Networks server web pages fully support operating as an SSL web site.

HandsFree Networks secured data communication is compiled with groundbreaking speed and accuracy, delivering zero-day threat neutralization



Action	Name	Sites	Privileges	Notifications Default Email Recipients	Reports Default Email Recipients
[edit] [delete]	above	Above & Beyond IT	Configure Machines Control Provision Remove Assets Control Downloads Control Updates	adonnini-notify@handsfreenetworks.com	adonnini-ereports@handsfreenetworks.com
[edit] [delete]	aco	DAMS	Configure Machines Control Provision Remove Assets Control Downloads Control Updates		

LOGIN AND PASSWORD SECURITY

HandsFree networks uses strong password authentication through logins and passwords. Passwords are hashed and encrypted and never travel across the networks. The login process includes security rules to temporarily block an ID when an incorrect password has been entered continuously in a row. In addition, you may limit login to specific IP range either on an individual or group basis, thereby restricting operation and access to HandsFree Networks server component.

HandsFree Networks server can only be accessed according to the permission assigned by the administrator to each operator. For example, an Administrator can decide which operator has access to features like specific DART configuration or remote control, and can further limit the available controls to allow operator to be a limited user (where one operator can see yet not take full control of the desktop).

All sessions use only an SSL connection regardless of the browser mode selected, thereby ensuring that transport layer encryption is utilized for the transmission.

SAFE CONNECTIVITY

HandsFree Networks utilizes TCP packets and standard port and is compatible with firewall and proxy server that performs network address translation (NAT). Connection can be established through a local area network or any other internet connection. This means that an Operator may be working outside the organization or from another country without a VPN connection and still connect to the company's services via browser to configure DART or take remote control from any other internet-connected workstation.

HandsFree Networks Support Automation solution functions 100% browser-based administrator access, using HTTPS protocols over standard Web port 443. Remote control sessions can be established using peer-to-peer connection with the same network. Ultra VNC is a remote control tool integrated with ReSOFT to provide administrator with secured access to remote devices and IT administrator can also assign a specific port to an operator.

AUTOMATED RC-FOOTPRINT REMOVAL

At the end of each remote control session, all active components of the remote control session are automatically removed from the end-user machine, thereby preventing any further unauthorized further access.

AUTHORIZED ACCESS CONTROL FOR REMOTE SUPPORT

Remote control sessions are always encoded with 256-bit end-end encryption standards. HandsFree Networks integrated remote access control always prompts customer approval before initiating and on-demand remote control. Once permission has

been granted by the customer, support professional can view a customer's computer as if they were sitting right in front of it.

During a remote control session, the customer can terminate screen sharing or screen viewing, decline downloads or files transfer and regain control of the desktop at any time. This ensures that the customer always has ultimate control on his or her own machine.

BLOCKING USER

To protect data security and leakage, ReSOFT includes blocking features that allow administrator to provide limited access or permanently block certain administration users from accessing and managing end-devices. The site administrator can block any user unilaterally by identifying the user's IP/port.

INTRUSION PROTECTION

Intrusion protection, a powerful and proven behavior-based protection incorporated into the ReSOFT support automation framework, provides an essential security protection component. HandsFree Networks offers come with advanced malware protection and latest self-healing proactive registry management technologies for spyware protection.

Whenever ReSOFT client detects a sequence of events corresponding to an attempted intrusion, or to an action not allowed (e.g. accepting incoming traffic on selected TCP/IP ports), it automatically runs one of the intrusion protection DART's for effective protection against malicious programs ensuring not only protecting from known threats but also provides zero-day threat neutralization.

For more information on the HandsFree Network Security features or Intrusion Protection functions, visit us at www.handSFreenetworks.com



HandsFree Networks Inc
1021 Main Campus Drive, Suite 300
Raleigh, NC 27606 (US)

HandsFree Networks Pvt. Ltd.,
4th Floor, Concorde Block, UB City,
Vittal Mallya Road, Bangalore-560001 (INDIA)

www.handSFreenetworks.com

HandsFree Networks and related HandsFree Networks Corporation logos are registered trademarks of HandsFree Networks Corporation. Copyright ©2009 HandsFree Networks. All rights reserved. All other company, product and brand names are trademarks of their respective owners.