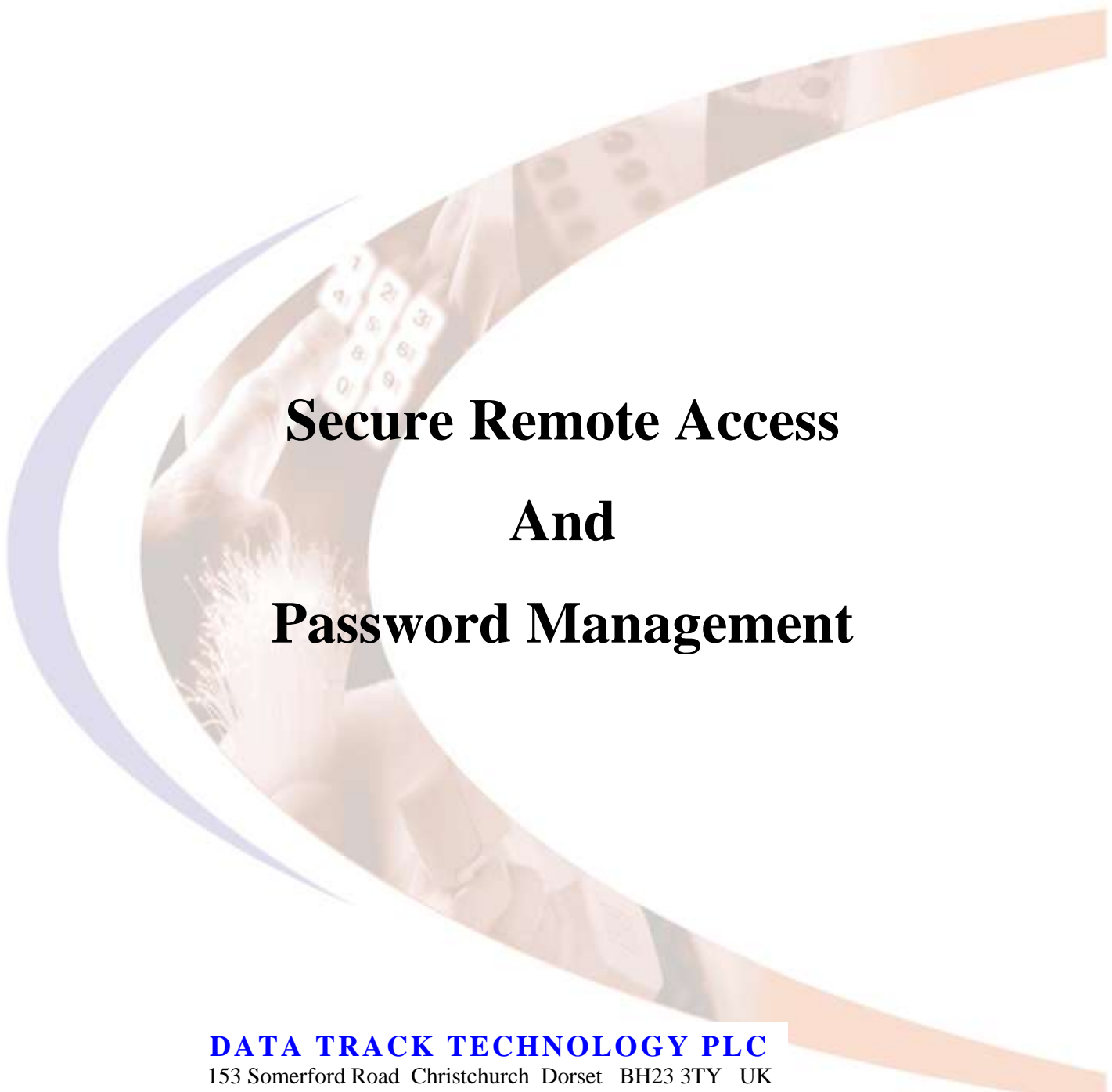




Communications • Management • Solutions

A large, semi-transparent, curved graphic element in shades of orange and purple frames the central text. In the background, a hand is shown typing on a computer keyboard.

Secure Remote Access And Password Management

DATA TRACK TECHNOLOGY PLC

153 Somerford Road Christchurch Dorset BH23 3TY UK

Tel: + 44 (0) 1425 270333

Fax: + 44 (0) 1425 270433

Email: sales@dtrack.com

Web site: www.dtrack.com

Contents

The Remote Access Problem 3

 SAMS is the Answer..... 3

Greater Security and Increased Efficiency 4

 For Enterprise Customers 4

 For a Maintainer..... 4

 Increased Security..... 5

 Training..... 6

Authentication..... 6

Resilience..... 6

Working with Trackers 7

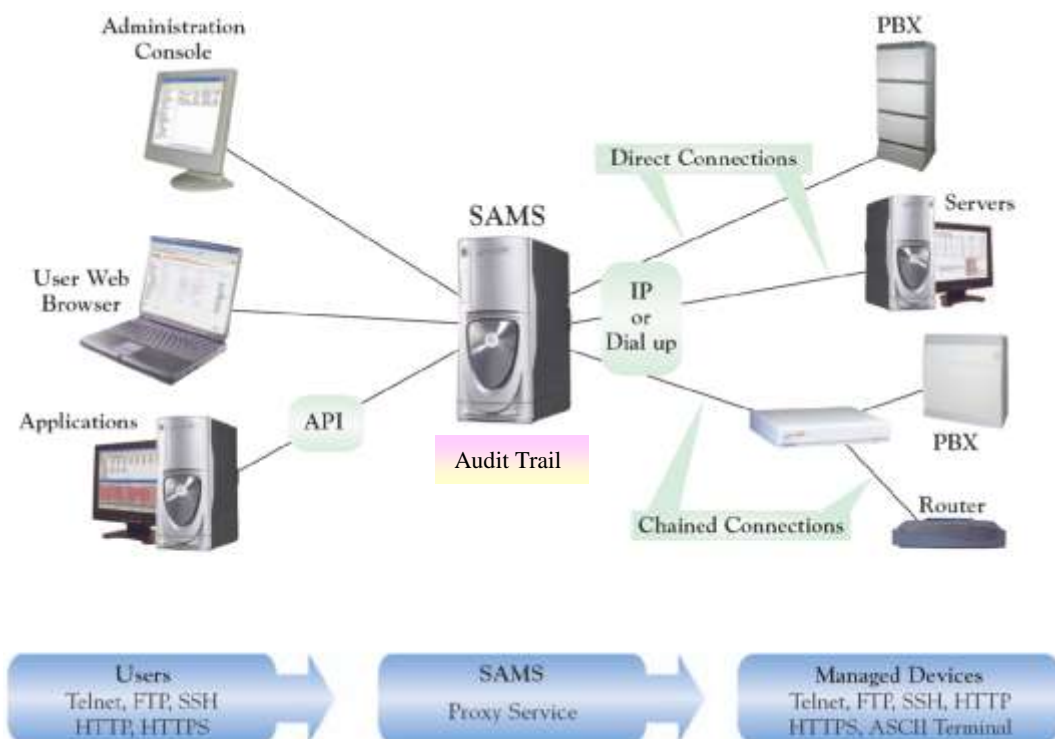
Conclusion 7

THE REMOTE ACCESS PROBLEM

Providing remote access to a variety of equipment, particularly where they are connected to a data network, raises significant security concerns and administrative problems for customers, service suppliers and equipment maintainers. Your remote users will need to know passwords to gain access; this is a security risk. Establishing connections require that your users have knowledge of various network protocols and proxy services; these can be complex. Your systems can be compromised by external hackers as well as internal staff; they require constant administration. You need to have an audit trail of who did what and when. What you need is a simple yet secure and auditable method of providing access to potentially large numbers of multi vendor equipment by users, engineers and administrators.

SAMS is the Answer.

The Tracker Secure Access Management System (SAMS) solves your problems by providing a centralised service that holds all your remote equipment password and connection information in a totally secure SQL database. It enables your users, administrators, engineers and applications to have secure remote access to managed devices, from a standard web browser, using IP or dial up connectivity. Users browse in to SAMS and get authenticated; they are then presented with a list of equipment they are permitted to access; connection is made with one click. They do not know equipment passwords, telephone numbers or IP addresses; it is simple, secure, fast and very efficient. SAMS proxies all the connections making life easier for users and keeps an audit trail of all activity making life easier for you.



GREATER SECURITY AND INCREASED EFFICIENCY

The use of SAMS brings many benefits for both enterprise customers and maintainers.

These benefits are outlined below

For Enterprise Customers

Greater security – the login credentials and connectivity details of all customer equipment will reside in the SAMS server. It will thus be easier for the customer to audit and approve a maintainer's security system.

Reduced Administration – customers IT staff will only need to provide external access to specific equipment on the network from one point i.e. the SAMS server. This will reduce their administration workload and associated costs.

Audit trail – SAMS will hold an audit trail of all remote access activity. In the event of a security breach it will enable the identification or elimination of remote maintenance as the source to be completed quickly and efficiently, saving time and cost.

For a Maintainer

Reduced Administration – SAMS will significantly reduce the administration overhead required to manage engineer and third party access to customer based equipment. Some of the increased efficiencies are outlined below

Adding equipment – without SAMS the existence of new sites or equipment must be notified to all users who require access to it. This information needs to include the login credentials and connectivity details. With SAMS all that is required is that the details are added to the SAMS database. .

Removing equipment – without SAMS all users have to be notified if equipment is removed. With SAMS all that is required is that the details are removed from the SAMS database.

Adding users – without SAMS a new user will need to be told of all the equipment that he has access to. This information needs to include the login credentials and connectivity details. With SAMS all that is required is that the user is given authenticated access to the SAMS database.

Removing users – without SAMS, when a user leaves all usernames and passwords of every device that they were able to access should be changed; this is an onerous task. With SAMS all that is required is that the user's details are removed from the SAMS database.

Changing Passwords – for security purposes it is generally considered good practise to routinely change equipment passwords. Without SAMS this can be a long manual process and all users have to be provided with details of the changes to only those sites and equipment to which they have access. With SAMS it is questionable whether the passwords need to be routinely changed. If policy dictates that they do, then there is no need to advise users of the changes as they do not need to know any login credentials.

Third party access – some equipment may be maintained by a third party supplier. These need to be given access to remote equipment either permanently or on a temporary basis. Without SAMS you will need to either provide a permanent login or change equipment passwords each time a third party has had access. With SAMS you can control third party access in exactly the same way as you control access by your own staff. This not only reduces the overhead of managing third party suppliers but can also reduce the time it takes to respond to an incident.

Increased Security

The use of SAMS will greatly increase the security of your operation, help you to audit activity, increase efficiency and reduce the cost of providing secure remote access. Some of these benefits are outlined below.

Audit trail – when an incident occurs it can be important to know if anyone has accessed a device and caused the problem. Without SAMS it is not possible to be certain of who did what and when. SAMS keeps a full audit trail that will allow you to quickly identify who did what and when. This includes the user and time with drill down to show data sent to and received from a device. The audit trail will also allow you to identify where additional training is required.

Security audit – in an increasingly security conscious world it is important that you can demonstrate that your systems meet ISO or similar standards. Without SAMS you need to give login credentials and connectivity details to individuals, some of whom may be contractors or work for third party companies. You will have to go to considerable lengths to convince your customers that your systems are secure. SAMS holds all login credentials and connectivity details in a secure central database; only administrators will have access to this information. This will allow you to more easily and cost effectively meet ISO standards and provide assurance to your customers.

Third party audit – where equipment is maintained by a third party, you will be held responsible for all their actions by your customers. Without SAMS you will have no idea what they have done and when. With SAMS you can produce a complete audit trail of activity including commands sent to and responses received from equipment.

Restricted access – some remote equipment, e.g. the Data Track Tracker, can be programmed to limit both dial up and IP access to both itself and devices connected to it. Without SAMS this can be very difficult and time consuming to implement; it may prove to be a practical non starter. With SAMS it is a simple task. All communications are channelled through the SAMS server so that connectivity can be limited to one CLI/ANI number and one IP address.

Training

Without SAMS, users will need some training on how to set up various connections from their laptop or workstation. These will include ASCII, Telnet, SSH, PPP, PPTP, FTP, HTTP, HTTPS and TCP. They will need to know which type of connection to set up for each equipment type and service. With SAMS they can use a standard browser to initiate all connections and services. SAMS will proxy the connection and use the correct protocol. This will greatly reduce the amount of training required by your users and greatly simplify the connection process.

AUTHENTICATION

It is important to ensure that access to the SAMS server itself is secure and that it fits within your existing security environment. SAMS can sit behind your firewall and you can use your existing security arrangements to control access to the application.

The SAMS system can use Windows Authentication which itself can be linked to a Radius server. For access by third party employees SAMS can force user password changes at regular intervals.

RESILIENCE

With all passwords and connection details stored on a single server and all remote access being forced down this route, it is important to consider what would happen in the event of a system crash. SAMS uses SQL as its database and this has a built in mirroring mode that allows all data to be replicated on another networked server. This can be located in a separate building for disaster recovery purposes.

Users browse into SAMS using a standard web browser. In the event of a total system loss the browser can be automatically diverted to the standby server. Using standard Microsoft Windows and SQL server anyone familiar with SQL environments will be able to provide such a resilient system.

WORKING WITH TRACKERS

SAMS can work directly with most remote equipment and customer environments. Where a greater degree of security is required or where access to serial interfaces is needed then SAMS can be used in conjunction with a Tracker unit.

The Tracker provides a powerful, flexible and reliable platform for the management of remote equipment via dial up, IP or VPN connections. With its access control tools, intelligent monitoring capability and range of connectivity options covering serial, modem, Ethernet and digital I/O, the Tracker allows you to manage all your on-site equipment from one access point. For further information on Tracker security see the separate Tracker Series Security Overview white paper.

CONCLUSION

It can be seen that introducing the Tracker Secure Access Management System into your organisation will produce many operational efficiencies. This will lead to reduced overheads, increased security and greater customer satisfaction. Being able to demonstrate an auditable security system for remote access will enable you to properly manage the remote access process.