Data Track Technology

+44(0)1425 270 333
email: sales@dtrack.com
website: dtt.dtrack.com/sams

Secure Remote Access and Password Management

Authentication - **A**uthorisation - **A**ccounting - **A**udit

Who needs access to your network devices? Administrators, users, engineers, 3rd party maintainers, contractors? How do you provide them with access yet keep device passwords secure? How do you audit what they have done?

Providing remote access to a variety of equipment, particularly where it is connected to your data network, raises significant security concerns and administrative problems. You will need to provide connection details and passwords to anyone who needs access to your equipment; this is a security risk. If they work for a third party, who are they? What happens if someone leaves, do you change the passwords on all your devices?

The Secure Access Management System (SAMS) is a single sign on solution that solves these problems. By using SAMS you will be able to reduce your administration costs, improve

SAMS will hold all your device credentials and connection information in a secure SQL database. It enables authenticated personnel to have secure remote access to equipment using IP or dial up connectivity, initiated via a secure web portal.

Users authenticate into the SAMS web portal; they are then presented with a list of equipment you have given them permission to access. A connection is made with just one click. SAMS launches the appropriate client application and logs the user on to the device.

Users do not need to know and are not shown equipment passwords, telephone numbers or IP addresses. SAMS proxies all the connections, making life easier for users, plus it keeps an audit trail of activity, making life easier for you.

Login to SAMS → *Click to connect* → *Audit activity*

Greater Security and Increased Efficiency

Simple, Efficient, User Control

You can control which of your network devices individual users or a group of users can view or access by providing each with a username/password profile. Make it easy for your users to locate a particular device. Group your remote equipment by location, maintainer, manufacturer, skill set etc or in any way you wish. When a user leaves, all you need to do is to remove their details from the SAMS database. There is no need to change the password on any of the devices they had access to.

Automate Regular Tasks

SAMS can run your scripts at regular intervals. These scripts can be used to automate regular administration tasks to increase efficiency and reduce operational costs. Examples of tasks that can be scheduled and automated include: changing the passwords of monitored devices, backing up the configuration of monitored devices, synchronising clocks on monitored devices (including daylight saving twice per year), plus any other tasks you can think of that can be automated.

Audit Activity

SAMS will hold an audit trail of remote access activity including commands sent to and responses received from equipment. In the event of a security breach you can identify the cause, saving you time and cost. SAMS will allow you to monitor the activity of third party maintainers and meet ISO standards.

Reduce Administration Costs

You will only need to provide access to specific network devices from one point. You can quickly and easily inform your users of site or equipment changes; all that is required is that the details are added or deleted in the SAMS database. Using SAMS will reduce your administration workload and associated costs.

Control Third Party Access

You can provide timed access to 3rd party maintainers with just one click. The connection will expire after the period you define and you will have an audit trail of what they did. Using SAMS will improve efficiency, increase security, provide an audit and reduce administration.

Improve Authentication

Host the SAMS application behind your firewall and use your existing security arrangements to control access to it. You can control logins via a username/password database, where password strength can be set as required. Users and third parties can be forced to change their passwords at regular intervals.

System Resilience

Multiple connection managers and web servers with IIS can be used to balance system load and provide for growth. SQL mirroring can be used to replicate the SAMS database onto other networked SQL servers. This ensures that there is no single point of failure in the system. A hot standby system can be located in a separate building for disaster recovery purposes, with SQL Log Shipping keeping the databases in sync.

Additional Security & Connectivity

SAMS will work directly with most network devices and in most environments. Where a greater degree of security is required or where access to serial interfaces is needed then use SAMS in conjunction with a Data Track manufactured Tracker unit. The Tracker allows you to manage all network devices from one access point, including alarm filtering and reporting.

System Requirements

SAMS requires or supports the following environment:

Operating System: MS Windows 2003 or 2008 R2 Server Standard and Enterprise
Web Server: IIS 6.0 for Window 2003 or IIS 7.0 for 2008 Server OS
Database: MS SQL Server 2005, 2008 or 2008 R2 Standard, Enterprise or Express