STAT - Identity Station

monitordynamics

STAT delivers up-to-date, wireless mobile credential validation for millions of cardholders - with or without database connectivity, and is powered by the SAFEnet Unified PACS Platform.

STAT Identity Stations are designed to allow authorized security personnel the ability to control access to any site, no matter how remote, with confidence by quickly authenticating and validating the roles, credentials and identities of individuals attempting to enter a specified area. Identity information on millions of individuals can be managed, using a handheld or ruggedized table device, without affecting performance, and without requiring a persistent connection to a server or other data source.

STAT was initially designed for use by the perimeter security guard, needing a FIPS 201 (HSPD-12) compliant mobile or handheld CAC, PIV or PIV-I, three factor authentication reader to validate the identities of all vehicle passengers. With integrated time & attendance capabilities, the STAT identity station quickly became a valuable tool for Federal Agencies to track personnel resources and more securely occupy guard stations at campus, base and agency perimeters.

STAT's mobile ID verification capabilities are critical when major emergencies, homeland security incidents, riots or natural disasters happen. These incidents may require the support of a number of federal, state, and local agencies, as well as private organizations, that do not collaborate with one another on a day to day basis. Faced with such a large and diverse group of first responders, accurate and efficient access control is very challenging. With STAT, unified into the SAFEnet System, individual cardholder privileges and identities are drawn from existing independent databases and published to STAT Handhelds and STAT mobile devices in a secure, fast and compressed data format.

As a smart card holder presents their credential, the information on the card is validated and the privileges displayed to the Security Officer, charged with controlling access and keeping facilities secure. STAT Identity Stations ensure that even when all computer and communication networks are down, the right people are able to gain access to the right areas at the right time.

STAT Identity Stations can deliver one, two or three factor authentication using Card, PIN and Biometric (finger) for true FIPS 201 compliance at every guard station, security checkpoint, gate entry or mobile emergency location.

STAT supports US Government issued smart cards including:

- FIPS 201-compliant PIV and PIV-I Cards
- First Responder Authentication Credential (FRAC)
- All Common Access Cards (CAC)
- Mariner Administrative Cards
- US State Department PKI Cards
- Transportation Worker Identity Credential (TWIC)
- Contact and contactless smart cards
- US driver's licenses

The Monitor Dynamics STAT Identity Station Product Line Includes:

STAT – HIS – Handheld Identity Station (One, Two or Three Factor Authentication)

STAT – HIS.TA – Unified Time & Attendance

STAT – MIS – Mobile Identity Station (Ruggedized Tablet PC with One, Two or Three Factor Authentication)

STAT – MIS.TA – Unified Time & Attendance

STAT

STAT - Identity Station

STAT Identity Station Basic Features:

Mobile validation - Perform immediate credential validation, anywhere, with or without network connectivity.

Large Database Storage Capabilities – Individual identity and access control information is stored on the STAT in a highly compressed, digitally signed identity and privilege list. With STAT, access and identity information on millions of cardholders from various agencies and organizations is readily available, anywhere, anytime.

Multiple, independent databases – Access privilege and identity data are sent to the STAT IPL Publisher from existing Government personnel databases. Participating independent organizations at the city, county, and national levels continue to maintain the identity and access privilege information in independent databases as they do normally.

Always current and updated – The STAT System synchronizes dynamically using standard wired or wireless connections when available. When an emergency strikes, or the STAT Identity Station is needed as a stand-alone solution, the device will always contain the latest data and a full electrical charge.

Continues working during network downtimes - STAT Identity Stations always store the most up-to-date identity and access privilege information in their local memory. This means that cardholders can be validated instantly without requiring a wired or wireless network connection to perform the operation, grant or deny access.

Multi-use device – The STAT Handheld or Mobile Identity Station is part of a Unified Security System. This means that the STAT can be used for various applications ranging from security at special events, mustering, and access control in remote environments where connectivity to outside networks is not possible.

Comprehensive reporting features – All events on the STAT Identity Station are logged and uploaded to the Central Station during synchronization times. These event logs can be used by security personnel to create comprehensive activity and after-action reports as required by supervisory personnel.

STAT - Handheld Identity Station

STAT - Features

- Runs on the latest MS Windows Operating System

- Meets IP67 standards for resistance to dust and liquids

- Can withstand total immersion in up to one meter (3.2 feet) of water

- Can withstand multiple one-meter drops to concrete or four-foot drops onto plywood

- Resistance to vibration and shock - equipped with 4GB (up to 32GB optional) SSDs (solid state disks) instead of hard disk drives

- Ports are "environmentally sealed by design," requiring no plastic caps or covers

- Optionally, sealed 10/100 Ethernet, RS232, and USB host ports may be added to the outside of the system

- Available with a three megapixel camera - option

- Built for challenging environments

STAT - Mobile Identity Station

www.monitordynamics.com

monitordynamics