ECSI International

IDMS® Interoperable Device Management System

Introduction

If you really want to do security right, you need a platform that unites your entire security system and allows for monitoring and control of every component through a single powerful interface within a framework built on extensibility and complete integration.

IDMS® unifies every component of a user's security system in a seamless manner, providing comprehensive and total control within a single, intuitive interface, supports virtually any component, sub-system or third-party security product on the market, and has been successfully deployed in Federal, Military and Energy Utility installations as well as Municipal, Educational, Healthcare and Commercial sites.

IDMS® will continue to meet your organization's security needs as technology evolves and your requirements change.

Unification Offers Simplification

When all of the data generated by every device in every facility throughout your entire organization comes together within a unified and well organized interface, the task of tracking, controlling, responding to events and maintaining records becomes much simpler. That's the power of unification — and a distinct advantage of the IDMS® platform.

IDMS® is designed and programmed to accommodate virtually any device or subsystem imaginable, not only within your security system, but throughout your entire enterprise. Whether it be alarms, doors, intercoms, cameras, building management devices, lighting controls, telephones, network devices, or software inputs, IDMS® can support virtually any electronic device or system operating on practically any protocol, giving you the highest possible level of unification and control.

This unification and control capability is especially powerful in organizations where multiple systems — such as IT, personnel management, network security, HVAC and even manufacturing systems — interact and share information. Each security device or subsystem is connected to the overall system through a “Portal,” and devices with similar characteristics can be grouped for easier management.

IDMS® also takes unification beyond the system level. If you have multiple IDMS® controlled security systems operating at separate facilities or campuses, a user with the proper permissions can connect to any or all of them simultaneously. Users can also control and manage multiple systems via any authorized workstation anywhere in the world.

Control Equals Better Security

If the security system itself is vulnerable to abuse, eavesdropping or other unauthorized activities, everything else is a moot point. That’s why IDMS® uses a robust collection of superior authentication and encryption methods to ensure that your system is secure.

The IDMS® Server lets you assign each user a number of profiles (user roles) that determine which functions the user can perform, which devices the user can access, and even the hours during which the user is authorized to operate the system. You can also take advantage of user group functionality to assign or change permissions for any number of users at once.

The IDMS® Server manages its own client connections, each of which is authorized through an assigned user profile with corresponding permissions. This role-based access control (RBAC) is the heart of user permissions.

All communications between the client and the IDMS® Server are authenticated and encrypted using the latest, most secure algorithms. The IDMS® Platform is compliant with the FIPS 140-2 Security Requirements for Cryptographic Modules as defined in that publication.

The Power of Synchronization

The scheduling functionality of IDMS® can be used to set automatic actions like turning on lights or bypassing certain alarms. The schedules you create, and the numbers or types of devices controlled by the schedules, are virtually limitless. The actions can be scheduled as repeating events to occur on a daily or weekly basis — or as one-time events at any date and time the user chooses, even years in advance.

With the development of a global marketplace, a growing number of organizations require a system that can accommodate globalization in a secure and logically managed environment. IDMS® provides time zone reconciliation and management so that users, devices, schedules, events, incidents and reporting can all be managed and logically presented to the user. There is no need for an operator to calculate or decipher time zone differentials on the system, as IDMS® manages this for you.

IDMS® also supports rules-based management with plugin components. These specialized software components make it possible to create customized functionality in your system, whereby an event or combination of events can trigger an action in another part of the system.

Core Capabilities & Portals

The IDMS® Unified Security Management Platform collects, analyzes, and unifies all available information from physical security devices and systems, as well as network monitoring and other software packages into a single comprehensive view for operator management and control. It provides situational awareness with video, audio (enabling call-on-incident and listen-in capability), real-time device status, advanced incident management, and conditional behavior functionality.

The IDMS® System Manager is the central server component for any IDMS® system. It securely manages user permissions, client connections, device/object linking, and timed events. IDMS® is available as a software-only package or as server hardware with pre-installed software, and is modular in nature, allowing easy integration into additional systems in the future. It can support an unlimited number of unique layout views and dashboards for an infinite number of users

The IDMS® System Manager software supports a rich set of core capabilities which are augmented by portals and optional software modules, and supervises administrator and user rights and permissions. Each user is assigned one or more profiles (roles), which encompass permissions for screen layouts (dashboards), schedules, workstation permissions, and device interactions. A flexible plugin-oriented system is utilized for user-authentication, supporting a wide array of methods. All communications between clients and the system manager are authenticated and encrypted, and are FIPS 140-2 compliant.

The IDMS® System Manager supports both physical and virtual devices within the limitations of the systems integrated and associated hardware. Devices may be associated with others to form a device group, for purposes of monitoring and control. User groups may be created to generate common profiles, properties, rights, and privileges. It also has the ability to handle control- and layout-based display synchronization across multiple clients via a common dashboard or layout. Clients support facility, location, and object mapping, including the display of situational awareness information on rendered drawings, complete with state-specific icons of each monitored component.

The system has the ability to support an unlimited number of conditional behaviors, allowing it to automatically perform actions when a given set of circumstances occur, based on device, system state, and time. Conditional behaviors can trigger a complex set of commands (known as macros) such as device commands as well as software user and third-party notifications. Macros are defined by the System Administrator.

Central to the unified security system are unified logging and reporting capabilities. IDMS® logs all system and user actions for later review, and reports are available for actions and states, devices, and incidents, and can also be associated with video recordings and cardholder access.

Portals are software components that provide the IDMS® System Manager with specific functionality and capabilities, such as the ability to control and monitor video, intercoms, and access control systems, among many others. ECSI International works with manufacturers to produce portals which can be created to support virtually any type of electronic system, using any type of communication format including IP-based, serial, or proprietary protocols. The IDMS® System Manager's core capabilities are augmented by plugin software modules, which can meet or exceed FERC (Federal Energy Regulatory Commission) standards.

Portal Features	Access Control	Video	Audio	Mass Notification	Workflow
Integrated 3rd Party Platforms	■	■	■	■	
Allow Unlimited Device & System Controls	■	■	■	■	
Provide Common User Interface	■	■	■	■	
User, Event & Schedule Triggered Recordings		■	■		
Allow Customized Layout	■	■	■	■	
Provide Unlimited Schedules	■	■	■	■	
Synchronize Devices with 3rd Party Platforms	■	■	■		
Retrieve Cardholder Information	■				
Provide Event History	■	■	■	■	
Allow Advanced Incident Management	■				■
Handle Alarms	■	■	■		
Provide Automatic Map Display upon Alarm	■	■	■		
Support Presets & Sequences		■	■		
Provide Display Control & Customization		■	■		
Support Multiple Manufacturers Concurrently	■	■	■	■	
Secure managed Content & Communication	■		■		
Offer Real-time Intercom Control			■		
Provide Recording & Playback with Control		■	■		
Offer Standards-based SIP & RTP Support			■		
Display Device Status as Icons on Maps, Text +	■	■	■		
Support Legacy Systems in Addition to Modern IP		■	■		
Provide Communication STatus to Operators				■	
Bridge Devices, Events & Policies to System				■	■
Provide Logging & Reporting	■	■	■		■
Offfer Workflow Step Printout Capability					■
Display Real-time Workflows + Current State					■
Allow Unlimited Process Scaling*					■
Create Triggers on Device States, Actions, Users					■
Allow Customized User & System Actions	■	■	■		■

**Subject to system harware limitations & licensing*

Advanced Interface Enables Control

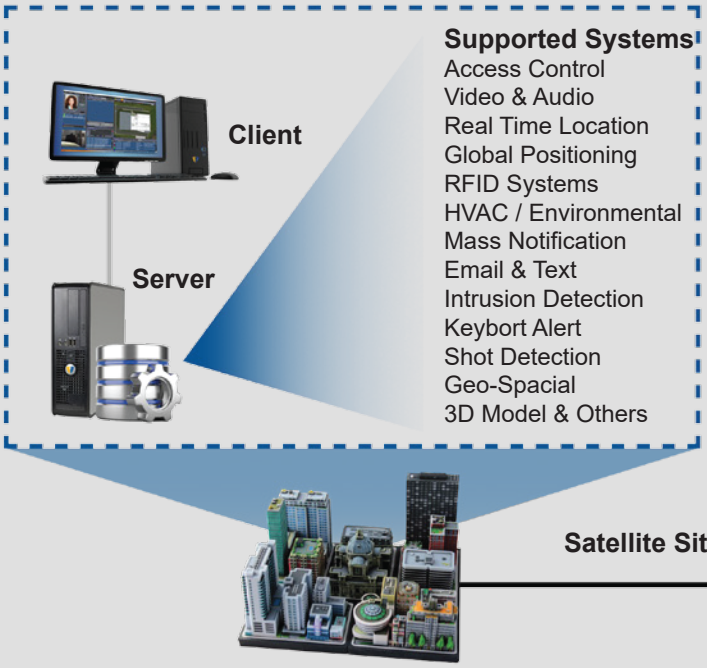
The IDMS® Graphical Client Workstation is highly intuitive, enabling users to navigate and control their security system with ease, speed and precision. Each device can be clearly represented by a device icon, hotspot or perimeter on any map format defined in the IDMS® map display packages.

The platform's basic map display package supports most standard formats, including AutoCAD® (.dwg and .dfx, including 3D) and file formats such as .bmp, .jpg, .gif and .tif. Optional packages provide support for a variety of 2D and 3D modeling formats, as well as GIS maps utilizing data from online servers or offline resources, including real-time data to track entities like storms, vehicles, assets or people. IDMS® is capable of supporting new graphic formats as they are developed and provides the ability to add features to support the needs of your application.

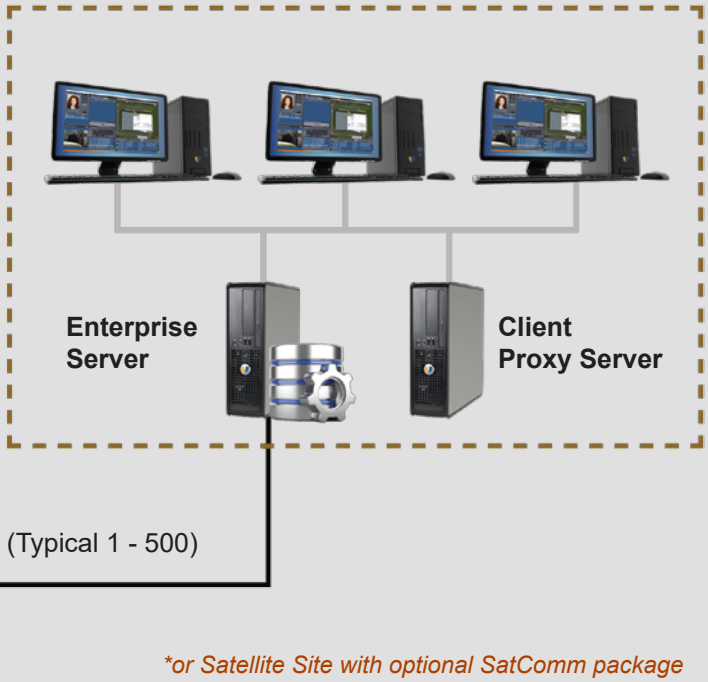
IDMS® uses advanced icon capabilities (through Icon Plugins) to help users visualize the security system and all its components from any perspective or zoom level. Available icon styles include vector-based icons that scale as the user zooms in and out, transparent and semi-transparent hotspots, and perimeters (e.g. fence segments) among others.

An extensive library of icons is provided and an icon editor for each Icon Plugin lets you create and edit the type of icon best suited to your system. A large library of controls, such as status lists, map windows, video windows and transaction lists are provided to meet the unique requirements of any user. In addition, custom controls can be provided. Screen layouts can also be configured as desired on multiple monitors.

IDMS® Single-Site* (Typical Setup)



IDMS® Enterprise (Typical Setup)



*or Satellite Site with optional SatComm package

Using a mouse, touchscreen or keyboard, the user can select the device from a sorted or searched list, drag and drop onto the map control for the auto call of an assigned map, or simply mouse over the icon to bring up a form indicating the device status or other information. A simple click accesses the controls specific to the device.

To view a live video feed from any camera, including a camera directly associated with a particular door, reader intercom or relay, the user simply drags the corresponding object to a video display window, or double clicks to pull the video to display, or does a video call-up with icon flyover.

The IDMS® platform also provides Enterprise-level operations with the ability to monitor and control multiple "satellite" standalone sites with Enterprise communication packages, concurrently as a centralized operation. IDMS® Enterprise supports continuation operations of satellite systems when off-line from the Enterprise server and includes multi-site aggregate report functions, as well as facilitating simultaneous cooperative management of alarms and incidents between local and Enterprise users.

TRACKING SYSTEMS **HVAC** **ACCESS CONTROL** **INTERCOM** **FACILITY**

FIRE **INTRUSION** **IP TELEPHONY** **VIDEO** **MASS NOTIFICATION**

Built-In Features Improve Security

Rather than just informing the operator of incidents like alarms, IDMS® offers advanced incident management capabilities that allow the operator to acknowledge or silence the alarm while keeping the incident active. Operator activities and devices associated with the incident are time stamped and logged. Detailed incident reports can be accessed at any time, and additional information can be added without compromising the integrity of previous content.

Users can access any event by calling up an incident list, clicking on a graphical object that corresponds to the event or selecting the event from a transactions window. Predefined entries are available to expedite reporting, but can always be overridden. When the incident is resolved, it can be closed, and the associated audio and video is saved with the report. Users with the proper permissions can reopen events for review and add data at any time.

In addition to standard incident management with user-defined, drop-down lists of pre-programmed responses, structured incidents are also provided for assigning SOPs (Standard Operating Procedures) to any event. These can be configured and assigned with stepped procedures and branched operations based on operator response. The structured incidents have no limitation on the number of steps and procedures that can be configured.

System Manager Functions

The IDMS® System Manager supports a host of key functions that are essential to the unified platform working hand-in-hand with your other integrated solutions, like gears in a well-oiled machine.

Some of the Highlights Include:

- Audio Management via SIP & RTP
- Scalability & Multi-site Capability
- Location-based Monitoring & Control
- Rights & Permissions for Admins & Users
- Profiles for Users, Schedules, Map Access & more
- Dashboard Layout Options with Dynamic Resizing
- Client Connection Management
- Unlimited Portals (Function-specific Software Components)
- Support for Physical & Virtual Devices, Groups & Privileges
- Natively Rendering Mapping in a Host of 2D & 3D Options
- Localized Time Formatting & Automatic Time Zone Reconciliation
- Programmable Actions with Assignable Priorities
- Unlimited Conditional Behavior Actions & Classifications
- Logs/Reports on Systems, Users, States, Actions & Devices
- Video Wall Support, plus Command & Control Displays
- Additional Login Methods such as Active Directory & Others
- Add-on Personal Record & Identify Management Solutions
- Add-on Visitor Identification Management Solutions
- Add-on GIS (Geographic Information Systems) Solutions

ECSI International | 790 Bloomfield Ave., Bldg C-1, Clifton NJ 07012 USA
(973) 574-8555 | ecsi@anti-terrorism.com | www.anti-terrorism.com