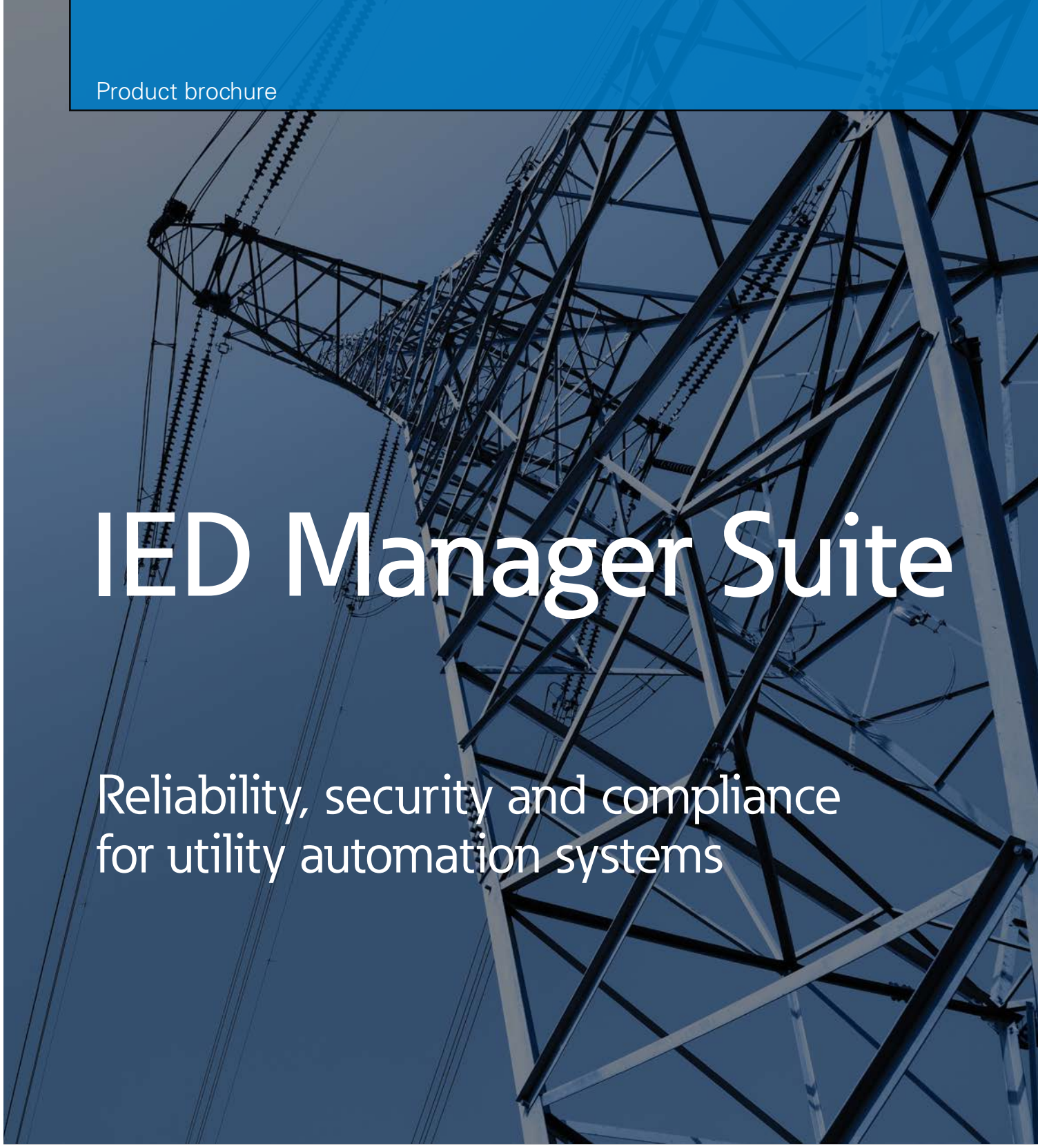
Product brochure



IED Manager Suite

Reliability, security and compliance for utility automation systems

Powering Business Worldwide

Eaton's IED Manager Suite (IMS)

provides power system operators with a complete suite of software applications to remotely manage all installed Intelligent Electronic Devices (IEDs) in the substation or distribution network.

Utilities are increasingly turning to integration and automation to enhance power system performance and reliability. Intelligent Electronic Devices (IEDs) are the cornerstone of their efforts. Installed throughout the utility, they protect the network, monitor critical equipment, detect problems, and prevent outages.

However, IEDs are produced by a variety of manufacturers and feature proprietary technologies as well as multiple protocols and data formats, with little or no security. This can create a maintenance and compliance nightmare.

IED Manager Suite (IMS) helps solve these problems. Not only does it integrate all IEDs into a cohesive, manageable whole, it also provides complete, enterprise-wide access to operational and non-operational data in a highly secure environment.

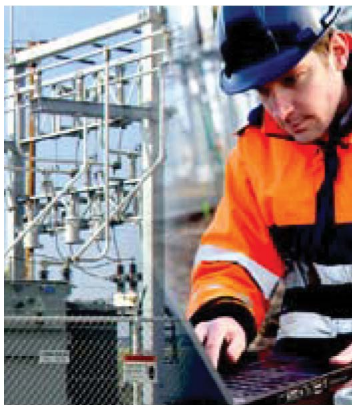
With thousands of IEDs being deployed in substations and in the distribution network, utilities are now faced with a growing management and compliance challenge. Operational expenses are growing as they strive to keep up with NERC CIP requirements, manage passwords, and deploy firmware updates.

IED Manager Suite provides utilities with the tools necessary to manage their fleet of intelligent devices in a secure and automated manner:

- Keep track of IED inventory
- Provide compliance reports and auditable logs
- Provide secure remote access
- Manage device configuration settings
- Manage passwords
- Manage firmware and settings updates
- Retrieve power system events, fault recors, SOE and oscillography
- Retrieve real-time operational data for asset monitoring and business intelligence

IED Manager Suite is composed of the following software modules:

- **Security Server**: Provides authentication and authorization services, ties in to Microsoft® Active Directory®
- **Enterprise Gateway and Data Bridge**: Manages communications with devices and publishes real-time data to control systems and data historians
- **Passthrough Manager**: Provides secure remote engineering access, auto-login, command filtering
- **Configuration Manager**: Retrieves device settings, monitors for changes
- **Password Manager**: Updates device passwords
- **Update Manager**: Updates device firmware
- **Event Manager**: Retrieves fault records, SOE, and oscillography



IMS Security Server

The IMS Security Server provides authentication and authorization services for all IMS modules, for SMP™ Gateway, and for managed devices.

Centralized access management for SMP Gateway and IED Manager Suite

Eaton's IMS Security Server provides centralized authentication and authorization services for IMS and SMP Gateway. It integrates with Microsoft® Active Directory® service to provide single sign-on capability to devices. When used with Passthrough Manager, users no longer need to know IED passwords and can connect to devices using their standard corporate credentials or IMS application credentials.

Additionally, IMS Security Server implements role-based access control, managing access by user, by group, by regions, by substation, and by IED.

The IMS Security Server leverages your existing corporate security infrastructure and provides centralized authentication and authorization services for field devices.

Key features

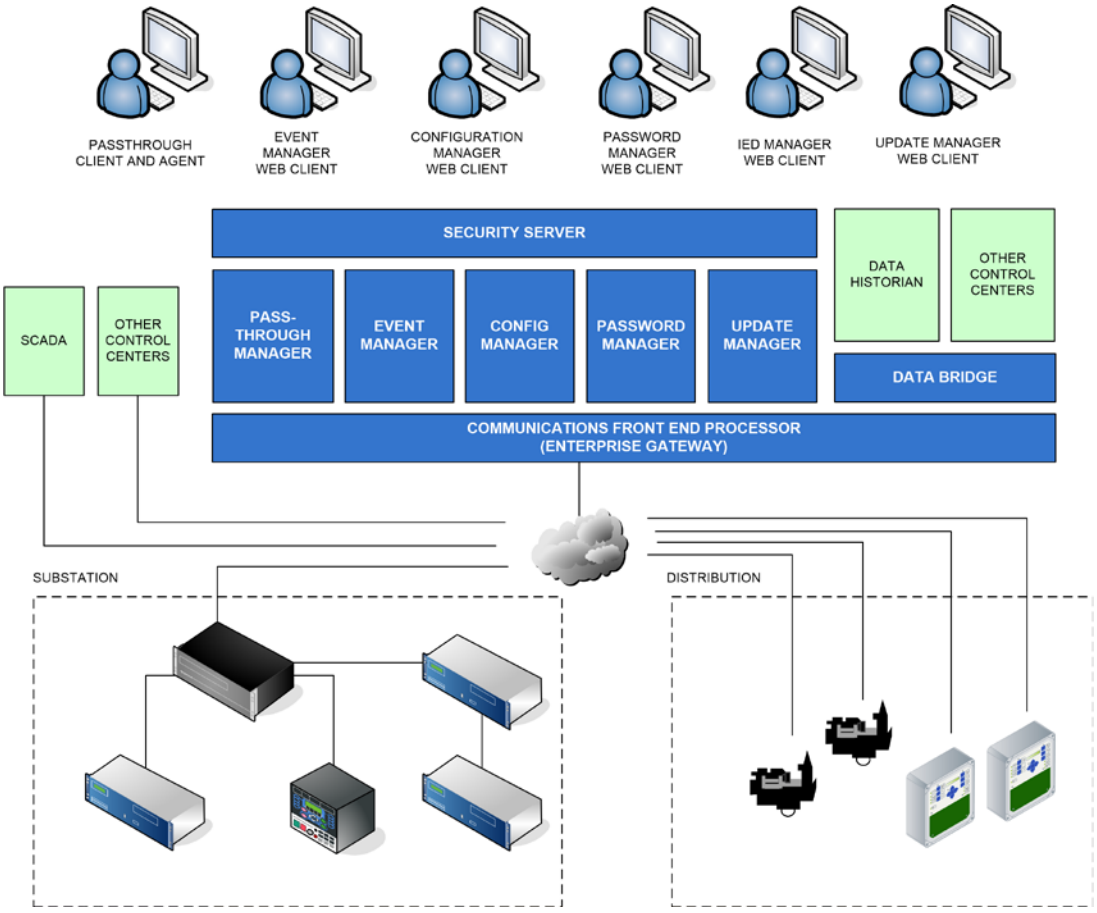
- Single sign-on and central authentication and authorization database
- Secure access to all IMS modules, Eaton's SMP Gateway, and all connected IEDs
- Simplified permissions management for supported Eaton's products
- Compliant with applicable NERC-CIP standards

Help comply with NERC CIP

Add, modify, and remove access rights from a central location, rapidly

- Implement central access monitoring and reporting
- Track user access to critical cyber assets

Automated IED management saves time and reduces errors



- Hide IED and gateway passwords from users, reducing the need for shared accounts
- Implement two-factor authentication for remote access to devices

Centralize user management

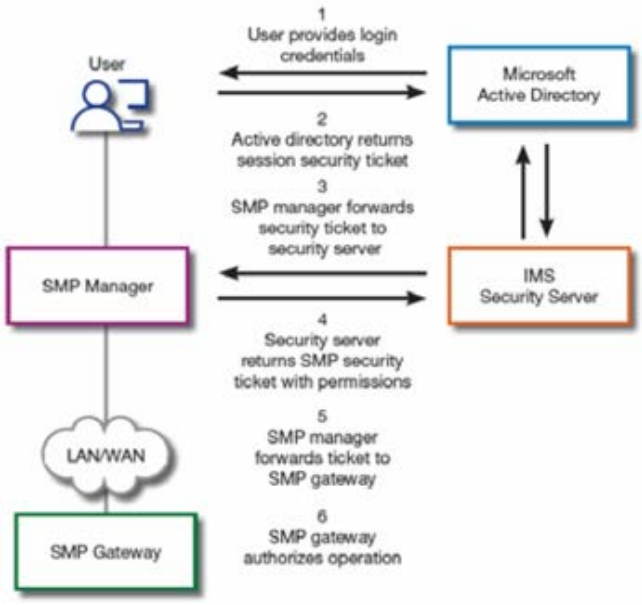
- Revoke access to all critical cyber assets with a single operation
- Create applicative accounts and set minimum password length and complexity requirements
- Grant access to individual applicative accounts, individual Microsoft® Active Directory® accounts, or Active Directory® groups
- Manage IMS permsions without needing Windows® operating system administrative permissions
- Review consolidated access logs

Centralize permission management and role-based access control

- Define groups of users
- Define groups of SMP Gateways and IEDs
- Define operations that groups can perform
- Assign users to groups to grant access to devices

Generate operation and compliance reports

- Detailed user and group permissions
- User activity report



IMS Passthrough Manager

IMS Passthrough Manager provides utilities with a secure remote maintenance and engineering solution.

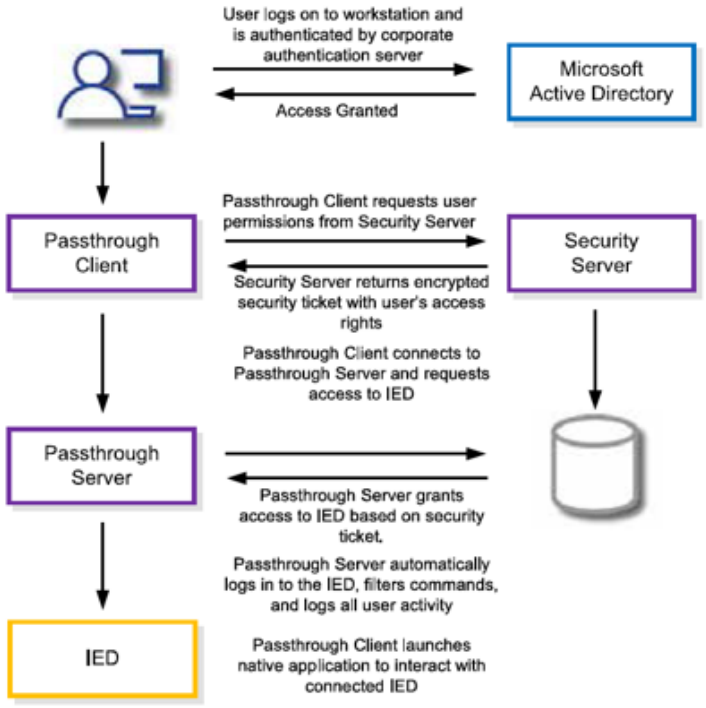
Secure, transparent access to remote IEDs

Eaton's Passthrough Manager provides users at the substation or enterprise level with secure NERC CIP compliant access to remote devices, using familiar vendor tools, as if they were connected directly to the IED.

Passthrough Manager is a client/server application. The Passthrough Client, installed on user workstations or on a shared application server, intercepts all data directed to the IED and securely forwards it to the server. The Passthrough Server provides authentication and authorization services, and forwards data to the IED, either directly, or through a secure communications link to the Eaton's SMP Gateway.

Helps meet NERC CIP requirements

- Provides intermediate device functionality as required by CIP-005
- Two-factor authentication support through Active Directory
- Individual user accounts
- Auto-login hides device passwords from users
- Command filtering prevents users from remotely changing IED passwords or sending harmful commands
- Secure TLS encrypted communications
- When used with Eaton's SMP Gateway, provides a secure connection from the enterprise to the substation Electronic Perimeter



Key features

Authentication and authorization

- Authentication through application user database or Microsoft® Active Directory® for single sign-on
- Centralized user permission management
- Access rights based on region and IED

Transparent remote access

- Users can connect to any IED to which they have been granted access
- Provide transparent remote access to IEDs from any application
- Supports devices using multiple IP ports
- Supports all common protocols HTTP, HTTPS, SSH, Telnet, etc.
- Connection settings, passwords, and communication encryption is preconfigured in Passthrough Manager: users connect as if they were in the substation

IMS Configuration Manager

The IMS Configuration Manager automatically retrieves and stores all IED configuration settings, detects changes to the baseline configuration, and notifies appropriate users. The IMS Configuration Manager provides utilities with a powerful tool to help meet NERC CIP configuration management requirements.

Centralized management of IED settings and firmware versions

Eaton's IMS Configuration Manager provides a secure browser-based user interface with the following functionalities:

- Monitor the configuration settings of Eaton's SMP Gateway and supported IEDs on demand, or on a scheduled basis
- Retrieve and store configuration files in a centralized database
- Define a configuration baseline
- Detect changes to configuration settings
- Notify system administrators of any detected change
- Maintain the history of configuration changes in an auditable database

With its advanced features, Configuration Manager provides utilities with a tool to simplify compliance with NERC CIP-010 requirements.

Key features

Retrieval, monitoring, and change detection

IMS Configuration Manager retrieves all available information from supported IEDs, not just ASCII text.

- Firmware and software version information
- Hardware information
- Patches and service packs
- Device settings and configuration

Configuration management, reporting, and notification

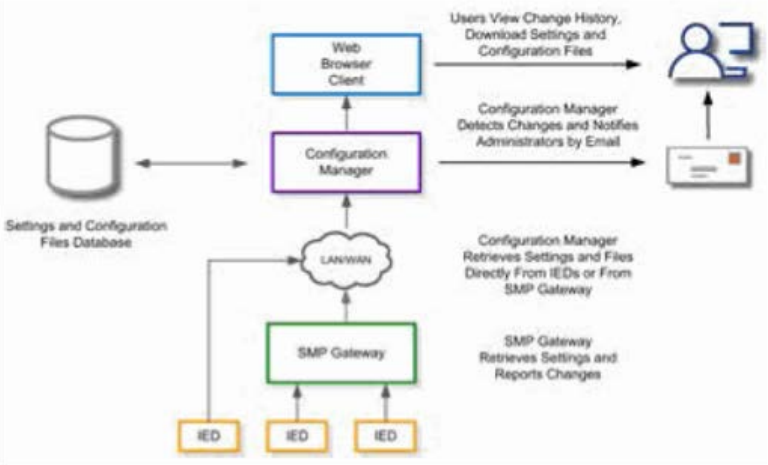
IMS Configuration Manager tracks device change history and notifies system administrators of any change to the baseline configuration.

- Define device baseline configuration
- Automatic email notification of detected changes
- View configuration changes
- View side-by-side comparison of settings from different versions or devices
- View device change history and generate reports
- Retrieve current or previous versions of configuration settings from the database

NERC CIP compliance functionalities

The following features help compliance with the NERC CIP-009 and CIP-010 requirements:

- Critical cyber assets configuration change history
- Configuration change automatic notification
- Configuration restoration and backup (simplified with the storage of all the information required to restore managed devices)



IMS Password Manager

IMS Password Manager provides a comprehensive set of tools and reports to manage IED passwords and help meet regulatory requirements.

Centralized management of IED passwords

Password management is a key requirement of all security programs such as NERC CIP. Compliance requires that utilities implement a process to:

- Manage inventory of devices and accounts
- Track and manage the use of shared accounts
- Generate compliant passwords
- Protect access to passwords
- Update passwords on a regular basis
- Provide compliance reports

Password Manager builds on Eaton's IED Manager Suite foundation to provide you with everything you need to implement your password management process:

- Secure encrypted storage of IED and Eaton's SMP Gateway passwords
- Simple-to-use Web-based management interface with granular access control
- Password length, complexity, and character set can be assigned for each device type and model
- Complete operational and compliance reports
- Fail-safe operation protects against password loss

Password Manager works the same way you do:

- Reduce the need for shared accounts by hiding device passwords through the use of Passthrough Manager auto-login capability
- Provide IED passwords to field personnel on a need-to-know basis
- Request a password change when work is done
- Print Current Passwords report for emergency use if communications fail
- Print Password Age report to plan and schedule password updates
- Utilize Password Usage and Password Change History reports to demonstrate compliance during audits

Password Manager provides you with a secure, easy-to-use Web-based interface:

- Navigate through regions, substations, devices, and accounts
- Secure role-based access control: users can only view devices to which they have access; users can only perform operations they are authorized to do

Authorized users can:

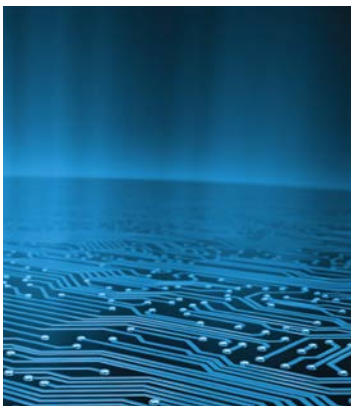
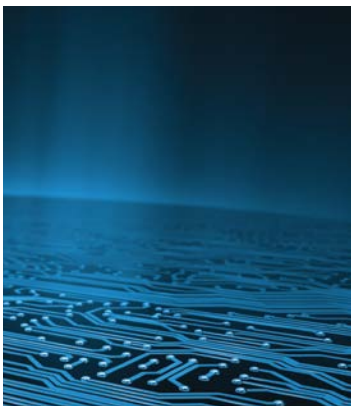
- View current password for any device account
- Copy password to clipboard
- Request password change for accounts, IEDs, or selected substation devices
- Print reports

With Password Manager, you are in control of the process. Every device type seems to have its own password policy, even when provided by the same manufacturer. You can select the best password for each device type. You can also select the device accounts or access levels you want to manage.

Password Manager is reliable. Lose the device password and remote access becomes impossible, requiring expensive field maintenance. Password Manager has been designed to handle all potential failure modes and provide fail-safe operations.

For increased reliability, passwords are managed centrally, not locally, and the database can be replicated to protect against data loss.



IMS Update Manager

IMS Update Manager helps keep IEDs secure and reliable by automating the process of updating device firmware.

Automating firmware updates

Frequent firmware updates have become a necessary fact of life to ensure the reliability and security of devices in the substation and distribution network. New features are being added, problems are being corrected, and vulnerabilities are regularly being identified.

Devices used in the distribution network are also subject to frequent changes to their settings, on a seasonal basis, or to address special conditions or issues.

Updating device firmware in a timely manner can also be mandatory for devices that have to meet the CIP-007 Security Patch Management requirements.

As the number of managed devices grows, updating firmware and settings manually becomes a tedious and error-prone procedure.

Update Manager is a companion module to the Configuration Manager that provides the following capabilities:

- Web-based user interface
- View current firmware version for supported devices
- Select devices and request update to new settings or new firmware version, immediately, or at a scheduled time
- View and print reports

Update Manager builds on the Eaton's IED Manager Suite foundation to provide you with everything you need to manage firmware and settings updates for supported devices.

Update Manager supports Eaton's SMP Gateway, CBC-8000 capacitor bank control, GridAdvisor™ Series II smart sensor, with more devices being added regularly.

Key features

- Simple-to-use Web-based management interface with granular access control
- Comprehensive Search capability by device name, model, and firmware version
- Select devices and group them by "batches" to be updated at the same time
- Select from available firmware versions
- Request update immediately, or at a scheduled time
- Automatically convert SMP Gateway settings and load the appropriate modules according to the software license
- Complete set of operational and compliance reports

IMS Event Manager

The IMS Event Manager provides corporate-wide access to power system events and fault records, SOE and oscillography from protection relays and DFRs.

Automated processing of power system events

Eaton's IMS Event Manager automatically retrieves event data from fault recorders and protection relays, notifies the proper users, and sends the event data along with the notification. Users can now have all the information they need to rapidly diagnose and act on problems, dispatch repair crews, and eventually restore service by remote connection to the affected device.

- Instant, automatic email notification of power disturbances
- Browser-based access to event history and event files

Features and benefits

Superior notification

- Automated email notification
- Event data automatically attached to the message
- Events can be sent to several users at a time

Remote access

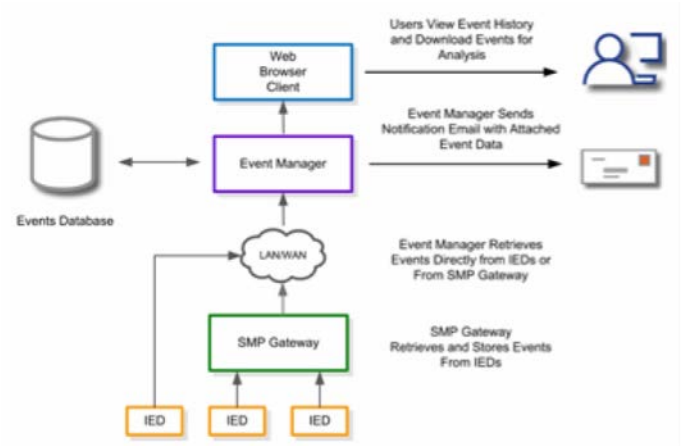
- Download event and waveform files using a Web browser, no need to connect to device
- Diagnose the event remotely
- Reduce substation visits

Efficient team management

- Dispatch alarms based on region and type of event
- Manage user access based on geography or teams
- Browser-based acknowledgement mechanism means one person takes ownership of the alarm

Event retrieval

- Automatic upon event occurrence, when using Eaton's SMP Gateway
- Scheduled at configurable intervals
- On demand via Web interface
- Keep event history for multiple-event analysis
- Comprehensive search capability
- Event grouping for simplified analysis
- Retrieved event data is stored in native format and converted to COMTRADE on demand



IED Manager Suite

Reliability, security and compliance for utility automation systems

Key system features

Architecture

- High performance multi-threaded architecture designed to support parallel operations on a large number of devices
- Built on industry-standard Microsoft® Windows Server operating system and Microsoft® SQL Server database
- Simple-to-use Web-based management interfaces with granular access control

Connectivity

- IMS supports devices accessible directly through an IP address, through a port switch, or supported data concentrators and gateways
- Supports up to four cascaded communications gateways
- Communications settings and timeouts are fully configurable to support slow data links

Comprehensive reporting capabilities

- Complete library of predefined reports for operations and compliance
- Comprehensive reporting capabilities built-on Microsoft® SQL Server Reporting Services
- Reports can be customized to meet your requirements

Comprehensive logging capability

- All user operations are logged
- All system operations are logged
- Logs are stored in the database
- Built-in Log Viewer application with searching and filtering capability
- Logs are simultaneously published to syslog server or SIEM for processing, monitoring, and storage

Supported device types

- AREVA MiCOM
- Eaton's Cooper Power series Form 6, CBC-8000, GE UR, GE SR
- SEL
- And many more

See "Devices Supported by IMS" document for a list of supported IEDs.

Supported gateway types

- Eaton's SMP Gateway
- SEL-2020 and SEL-2030
- NovaTech™ Orion

Server software requirements

Operating system

- Windows® Server 2008 R2
- Windows® Server 2012 R2
- Windows® Server 2016

Web server

- Microsoft® Internet Information Services (IIS) Version 6.0 or later

Database

- MS SQL Server 2008 R2
- MS SQL Server 2012
- MS SQL Server 2014
- MS SQL Server 2016

Client software requirements

IMS Management Console is a Windows® client application that runs on the IMS server.

- Windows® Server 2008
- Windows® Server 2012
- Windows® Server 2016

IMS Passthrough Client and Agent run on a user workstation or shared application server.

- Windows® 7
- Windows® 8.1
- Windows® 10

Server hardware requirement

IMS hardware requirements depend on the number of monitored IEDs and the number of event and configuration files stored for each of these IEDs.

The following are typical minimum requirements.

Processor type

- Minimum: Intel™ Core 2 or equivalent or faster

Processor speed

- Minimum: 1.0 GHz
- Recommended: 2.0 GHz or faster

RAM

- Minimum: 4 GB
- Recommended: 16 GB or more

Disk

- Minimum: 100 GB
- Recommended: 500 GB with RAID, SAN or NAS

Virtualization support

- Microsoft® Hyper-V
- VMware® ESX and VMware ESXi
- Citrix® XenApp

For Eaton product information, call 1-877-834-0009 or visit: www.eaton.com/smartgrid

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Eaton
Electrical Automation Solutions Division
3033 Campus Drive, Suite 350N
Minneapolis, MN 55441
United States
Eaton.com/SmartGrid

Printed in USA
Publication No. BR913001EN
January 2019

Follow us on social media to get the latest product and support information.

Powering Business Worldwide