Программные решения для промышленных сетей критической инфраструктуры CROSSBOW

Описание

По вопросам продаж и поддержки обращайтесь:

Алматы (727)345-47-04
Ангарск (3955)60-70-56
Архангельск (8182)63-90-72
Астрахань (8512)99-46-04
Барнаул (3852)73-04-60
Белгород (4722)40-23-64
Благовещенск (4162)22-76-07
Брянск (4832)59-03-52
Владивосток (423)249-28-31
Владикавказ (8672)28-90-48
Владимир (4922)49-43-18
Волгоград (844)278-03-48
Вологда (8172)26-41-59
Воронеж (473)204-51-73
Екатеринбург (343)384-55-89
Иваново (4932)77-34-06
Ижевск (3412)26-03-58
Иркутск (395)279-98-46
Казань (843)206-01-48
Калининград (4012)72-03-81
Калуга (4842)92-23-67
Кемерово (3842)65-04-62
Киров (8332)68-02-04
Коломна (4966)23-41-49
Кострома (4942)77-07-48
Краснодар (861)203-40-90
Красноярск (391)204-63-61
Курск (4712)77-13-04
Курган (3522)50-90-47
Липецк (4742)52-20-81
Магнитогорск (3519)55-03-13
Москва (495)268-04-70
Мурманск (8152)59-64-93
Набережные Челны (8552)20-53-41
Нижний Новгород (831)429-08-12
Новокузнецк (3843)20-46-81
Ноябрьск (3496)41-32-12
Новосибирск (383)227-86-73
Омск (3812)21-46-40
Орел (4862)44-53-42
Оренбург (3532)37-68-04
Пенза (8412)22-31-16
Петрозаводск (8142)55-98-37
Псков (8112)59-10-37
Пермь (342)205-81-47
Ростов-на-Дону (863)308-18-15
Рязань (4912)46-61-64
Самара (846)206-03-16
Санкт-Петербург (812)309-46-40
Саратов (845)249-38-78
Севастополь (8692)22-31-93
Саранск (8342)22-96-24
Симферополь (3652)67-13-56
Смоленск (4812)29-41-54
Сочи (862)225-72-31
Ставрополь (8652)20-65-13
Сургут (3462)77-98-35
Сыктывкар (8212)25-95-17
Тамбов (4752)50-40-97
Тверь (4822)63-31-35
Тольятти (8482)63-91-07
Томск (3822)98-41-53
Тула (4872)33-79-87
Тюмень (3452)66-21-18
Ульяновск (8422)24-23-59
Улан-Удэ (3012)59-97-51
Уфа (347)229-48-12
Хабаровск (4212)92-98-04
Чебоксары (8352)28-53-07
Челябинск (351)202-03-61
Череповец (8202)49-02-64
Чита (3022)38-34-83
Якутск (4112)23-90-97
Ярославль (4852)69-52-93

Россия +7(495)268-04-70
Казахстан +7(727)345-47-04
Беларусь +(375)257-127-884
Узбекистан +998(71)205-18-59
Киргизия +996(312)96-26-47

эл.почта: rmi@nt-rt.ru || сайт: https://ruggedcom.nt-rt.ru/

RUGGEDCOM CROSSBOW is a proven Secure Access Management solution designed to provide cybersecurity compliance for industrial control systems.

Contents

Introduction

RUGGEDCOM CROSSBOW is a proven enterprise-class solution for secure remote and local user access and management of intelligent electronic devices according to recognized cybersecurity standards, e.g., NERC CIP and IEC 62443. It allows for the automation of passwords, firmware, configuration, and data management of field assets and provides a comprehensive reporting mechanism for regulatory compliance. Operators of industrial control systems in critical infrastructure, such as electric power utilities, renewables, rail, oil and gas, etc., can benefit from the flexibility, scale, and most importantly the security offered by RUGGEDCOM CROSSBOW.

RUGGEDCOM CROSSBOW is designed to be simple, economical, and intuitive enough to be operated by large numbers of personnel according to, and without inhibiting, their normal duties across functions such as:

- Asset condition monitoring
- Event response and investigation
- Maintenance (including maintenance performed by vendors)
- Control, protection, and telecommunications engineering

Challenges for operators of industrial control systems in critical infrastructure

Increasing digitalization of industrial control systems:
Automation systems in critical infrastructure industries allow for remote management and control of critical field assets, providing significantly higher operational efficiencies but increasing the risk of cyber-attacks, thereby driving the need for a reliable yet cost-effective access management solution.

Complexity and scale of managing critical assets with evolving security requirements:
Field devices and intelligent electronic devices (IEDs) designed for high availability and reliability in harsh environments have fundamental security requirements. These multi-vendor assets are distributed across remote locations, requiring significant time, effort, and cost for engineering personnel to manually perform maintenance and management activities on site.

Compliance with OT cybersecurity standards and regulations:
Cybersecurity standards mandate Bulk Electric Systems to support preventative measures to block unauthorized access to critical assets and provide timely notifications to a centralized location. All activities performed by authorized personnel must be logged and reported as per the governing cybersecurity standards.

Benefits

RUGGEDCOM CROSSBOW is a comprehensive and scalable solution with a seamless configuration environment to allow users to securely access intelligent electronic devices for remote maintenance, configuration, and data retrieval – thus meeting the needs of industrial and utility asset owners for cybersecurity compliance. Its ability to provide role-based access control makes it an essential tool for any IED-based application for:

- Utilities (electricity, renewables, water, gas)
- Transport control systems (rail, ITS)
- Industrial and mining applications
- Building/site management systems

Ease of administration

- Vendor-agnostic design that works with all common IEDs and field devices
- Central point of administration and management of thousands of IEDs and hundreds of users
- Structured view of IEDs (region/substation/gateway) to provide a comprehensive view of asset hierarchy
- Dashboard with essential system information
- Grouping of devices and users
- Configurable sub-admins
- Spreadsheet engineering via bulk import/export
- Automated database management to control database growth

Secure solution for cybersecurity compliance

- Enables compliance with NERC CIP and IEC 62443 standards for remote IED access, user activity (keystrokes) logging, and data privacy
- Provides a complete set of one-click NERC CIP compliance reports
- Integrates with Active Directory, RSA SecurID, and other enterprise authentication solutions to provide strong two-factor authentication
- Provides individual user accounts with highly configurable permissions
- Offers role-based remote access control of field assets
- Logs and reports all system activities and security events
- Blocks and logs specified IED commands on a per-device type/per-user basis
- Provides optional encryption between server and remote facility
- Filters sensitive information from appearing in the logs with configurable settings
- Offers automated Asset Discovery function through a licensable integration with third-party IDS to scan the network for previously unknown devices

Scalable and flexible architecture

- Client-server or "clientless" architecture using virtual desktops
- High-availability option with server clustering
- WAN or dial-up access
- Local substation access control through RUGGEDCOM CROSSBOW Secure Access Manager – Local (SAM-L) and CROSSBOW Station Access Controller (SAC)

Advanced automation functions for asset management

- Automated password management
- Automated verification of configuration and firmware versions
- Scheduled report generation
- Automated file retrieval (fault files and sequence of events files) from IEDs

Ease of accessibility

- Allows for event information distribution to external tracking systems
- Offers file export service to transmit files retrieved by DATA and Config CAMs
- Provides external CAM (CROSSBOW Application Module) triggered via External Database Integration Service

Comprehensive multi-vendor device support

- Siemens, SEL, GE, ABB, Belden, Alstom, Novatech, Satec, Beckwith, Cisco, Cooper, Bitronics, other

Ease of integration

REST API (Application Programming Interface) provides a unified and effective way for the integration of 3rd party applications and allows for:

- Access to basic device information
- Access to files associated with devices
- Ability to trigger CAM operations on the device

System architecture

RUGGEDCOM CROSSBOW's client-server architecture is designed for any large, medium, or small-scale industrial operator or utility to easily and securely manage remote connectivity to its entire population of field IEDs. User access is role-based, and device credentials and network topology details are obfuscated from the users. It allows IED maintenance applications in the control center to remotely communicate with its associated IEDs as if the users were directly connected to the device.

Key components

RUGGEDCOM CROSSBOW Secure Access Manager Primary: SAM-P

RUGGEDCOM CROSSBOW Secure Access Manager Primary is a central system component through which all remote connections are made, and it is the only trusted client source for the IEDs. It runs on an enterprise-grade Windows server platform, either on a dedicated hardware or a virtual machine, and uses Microsoft SQL Server database for data storage. RUGGEDCOM CROSSBOW SAM-P enables role-based access control (RBAC) by verifying the authenticity of the user, either through a personal username and password (basic security) or through interaction with a corporate security system (strong authentication). After verification it allows the logged-in user to view all available devices. When a device is selected for connection, RUGGEDCOM CROSSBOW SAM-P establishes a secure communication path to the device, either directly or through one or more remote gateways. The RBAC is configured during the installation to control individual users and user groups have varying arrangements of read/write access to IEDs, which can be controlled by region/facility/IED or even command level. The strong authentication option allows for the integration of the user identification and permissions to be linked to the corporate system such as Active Directory, RSA SecureID, or a RADIUS server. It requires all users to be authenticated by an external service.

Alternatively, the Application Virtualization Server architecture also allows for central management of all native IED applications via a virtual desktop, such as Citrix XenDesktop®, eliminating the need for client software on the user's desktop.

RUGGEDCOM CROSSBOW Client

It is the primary interface to access devices based on user privileges, launch connection sessions, and access device-related tasks and reports. It redirects all communications to/from the device maintenance and/or configuration application through either a network proxy or a virtual serial port. It connects to RUGGEDCOM CROSSBOW SAM-P through a secure SSL connection.

RUGGEDCOM CROSSBOW Station Access Controller: SAC (optional)

RUGGEDCOM CROSSBOW SAC offers local and emergency IED connectivity in case the connection to the centralized RUGGEDCOM CROSSBOW SAM-P is down. It provides the same level of command control and logging when a user is physically present in the station and is synchronized with the SAM-P. RUGGEDCOM CROSSBOW SAC may run directly on ROX, i.e., on the RUGGEDCOM RX1500/RX5000 Multi-service Platforms, or on the RUGGEDCOM APE1808 module with a Windows operating system.

RUGGEDCOM CROSSBOW Secure Access Manager Local: SAM-L (optional)

RUGGEDCOM CROSSBOW SAM-L is designed to be deployed in local facilities. Not only does it provide local and emergency connectivity, e.g., RUGGEDCOM CROSSBOW SAC, but it also offers advanced automation functionalities, such as password management automation and CROSSBOW Application Modules (CAMs). RUGGEDCOM CROSSBOW SAM-L is synchronized with RUGGEDCOM CROSSBOW SAM-P and may run on the RUGGEDCOM APE1808 module or any industrial personal computer deployed to the facility and running on the Windows operating system.

Enterprise integration

Most customers of RUGGEDCOM CROSSBOW will have their own enterprise security systems, such as Active Directory, RSA, or RADIUS. RUGGEDCOM CROSSBOW can integrate and make use of these components for authentication. The use of an SQL server is required by RUGGEDCOM CROSSBOW SAM-P to store its database. It is recommended that the operator makes use of their own enterprise SQL servers to hold this database.

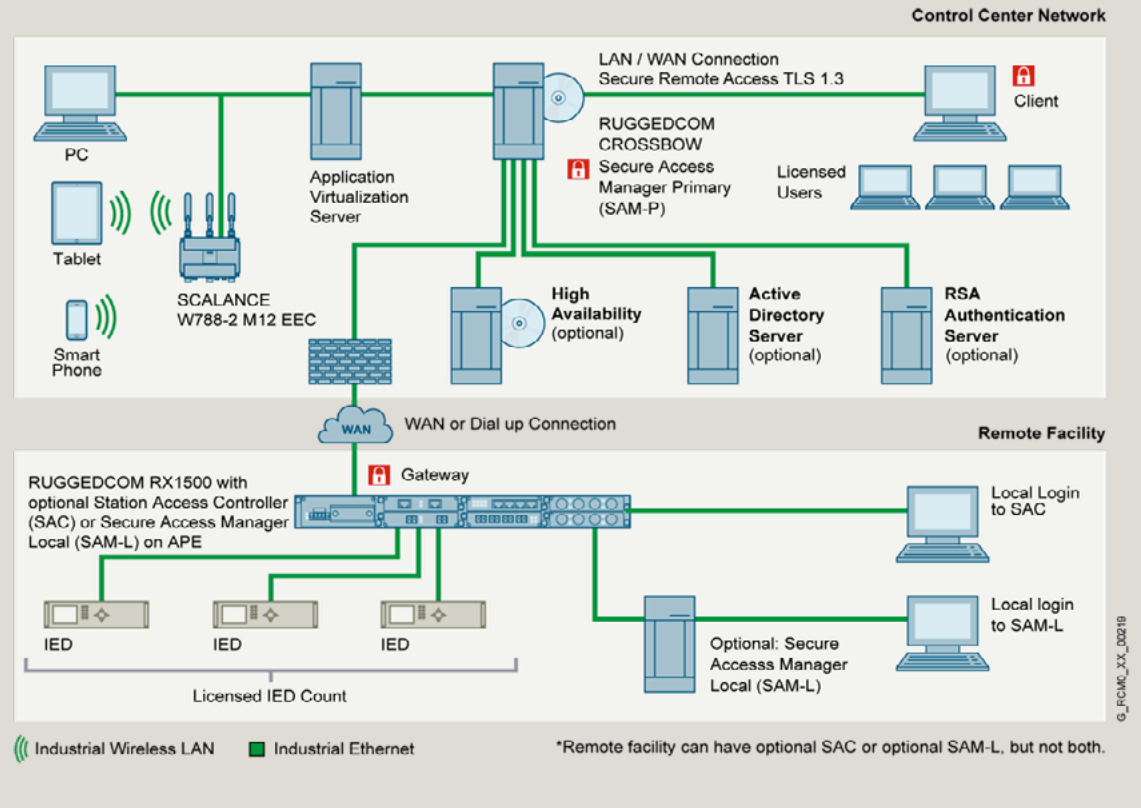
Ensuring high availability – server clusters

The RUGGEDCOM CROSSBOW server can be licensed to make use of multiple servers configured as a cluster. This allows multiple servers to exist as a single entity, enabling more users to utilize the system at the same time and faster processing of automated tasks, such as fault record retrieval.

The SQL server(s) may also be configured in a cluster for high availability. The primary DB ships data to the mirror in real-time. A typical cluster may contain three SQL instances: the primary DB, the mirror DB, and a witness server (optional).

Typical workflow

RUGGEDCOM CROSSBOW is specifically designed to be intuitive and enhance users' normal activity. After logging-in to the central SAM-P server, the user is presented with a simple directory structure displaying regions, substations, or remote sites and devices to which that user has been granted access by the administrator. From there, the user clicks on a chosen device to establish a connection. After a connection to the end device is established, the user's RUGGEDCOM CROSSBOW Client application launches the specified application to open an interface with the device (SSH, Telnet, HTTPS, etc.). Depending on the type of application and end device, communication can take place either using a virtual serial port (for serial devices or, in some cases, for Telnet/SSH connections) or a network proxy endpoint (for network devices) provided by RUGGEDCOM CROSSBOW Client to the application.



Server and client requirements

Software requirements*

- Microsoft.NET Framework v4.6.2
- Microsoft SQL Server
  Microsoft SQL Server 2017/2017 Express
  Microsoft SQL Server 2019/2019 Express
- OLE DB (latest version)
- Microsoft Visual C++ 2015-2022 Redistributable
- Microsoft Excel or equivalent
- PDF Viewer
- Command Line File Compare Utility

Server hardware (SAM-P) requirements

Siemens recommends that a dedicated server be provided for RUGGEDCOM CROSSBOW. Other closely related applications – such as Microsoft SQL Server – may be hosted by this server as well, but unrelated applications should not.

The following details the minimum hardware requirements for a RUGGEDCOM CROSSBOW Server:

Component	Specification
CPU	x86 Compatible, 12-core, 2.40 GHz or faster
RAM	16 GB or more
Disk	1 TB
Operating System	Windows Server 2016 (64-bit) Windows Server 2019 (64-bit) Windows Server 2022 (64-bit)

* Requirements may change for the new RUGGEDCOM CROSSBOW release.
Please check the RUGGEDCOM CROSSBOW Server guide for additional information.

Client/Windows (SAC/SAM-L) hardware requirements

Workstations running RUGGEDCOM CROSSBOW Client, Windows SAC or SAM-L should meet the following minimum requirements:

Component	Specification
CPU	x86 Compatible, 6-core, 2.40 GHz or faster
RAM	8 GB or more
Disk	500 GB
Operating System	Windows 10 Windows 11 Windows Server 2016 (64-bit) Windows Server 2019 (64-bit) Windows Server 2022 (64-bit)

System components

Component options included by default

Dashboard
The system dashboard provides system administrators with a high-level overview of the RUGGEDCOM CROSSBOW system. It displays a summary of current alerts, device status, user and device connections, event counts, and other system-level summary information. Each category is displayed in its own panel within the categories pane.

Password management
RUGGEDCOM CROSSBOW can change supported devices' passwords either to a specified password or a randomized password, based on what that devices firmware supports. Passwords belonging to a specific facility, device group, device family, or device type can be changed in a single operation. Authorized users may see/know a device's credentials. Credentials are obfuscated from all other users.

Reporting engine
RUGGEDCOM CROSSBOW allows users to generate a variety of reports based on criteria, such as incident type, location, device(s), and user(s). Customized reporting criteria can be saved for future use. Once generated, reports can be viewed in RUGGEDCOM CROSSBOW Client and/or sent to users via email.

Bulk importer
Information related to devices/gateways in the RUGGEDCOM CROSSBOW database can be imported and exported using RUGGEDCOM CROSSBOW's bulk import/export feature. This feature allows an administrator to export the data from the RUGGEDCOM CROSSBOW database into a Microsoft Excel spreadsheet and modify it as needed and/or import modified data from the spreadsheet back into the database. Thus, creating new regions, facilities, and devices and/ or modifying the settings of existing ones.

Device Type Definition Tool (DTDT)
CROSSBOW DTDT allows RUGGEDCOM CROSSBOW administrators to create and install their own custom device types. While RUGGEDCOM CROSSBOW features a variety of pre-defined device types that can be cloned and then customized, the DTDT allows administrators to create entirely new device types that best meet their requirements.

Background logger
This feature can be run in the background of the RUGGEDCOM CROSSBOW server. It captures internal log messages to assist in debugging and analyzing field issues.

REST API
REST API provides a unified interface to allow external applications to access device-specific information and trigger CAM operations on a device or group of devices.

Component options for licensing

RUGGEDCOM CROSSBOW Application Modules (CAMs)
CAMs are separately licensed "plug-ins", which can be added to a default functionality. CAMs are run by the CROSSBOW scheduler and may be run on demand or on a periodic basis, scheduled at specific time intervals as required.

The SAM-P server can be configured to run multiple CAM operations in parallel and on a redundant server. Each member of a RUGGEDCOM CROSSBOW cluster will process tasks in the scheduler queue.

Connectivity CAM
Connectivity CAM is designed to automate the monitoring of RUGGEDCOM CROSSBOW's ability to connect to the devices in its database. This ensures that any given end device remains available for other RUGGEDCOM CROSSBOW communications (e.g., end-user connections, other CAMs, etc.) and to alert a user when it is not.

Data CAM
Data CAM automates the collection of fault and event data from the targeted devices/gateways. The following data can be retrieved from IEDs and stored in the RUGGEDCOM CROSSBOW database:

- Oscillography files
- Target status
- Sequence of Events (SOE) data
- Fault reports

Firmware version CAM
Firmware version CAM connects to managed devices, reads the firmware version, and compares the devices' current value to the values expected for that device. Any variation from the baseline results in an alert.

Configuration management CAM
Configuration management CAM connects to managed devices, reads their settings, and compares them to their latest approved baseline. Any variation from the baseline results in an alert.

Time compare CAM*
Time compare CAM connects to managed devices, reads the current timestamp, and compares it to the system time on the RUGGEDCOM CROSSBOW server. Any variation from the defined baseline results in an alert.

* Enabled for GE UR relays and SEL relays

Nozomi Networks Guardian™ IDS (Intrusion Detection System) integration option
This license automates asset discovery by retrieving data from an existing Nozomi Networks Guardian™ IDS and populates the RUGGEDCOM CROSSBOW database with end devices that were not known earlier. This helps to keep track of the new and/or transient devices connected to the network and maintain an up-to-date asset inventory.

Nozomi Networks CMC (Centralized Management Console) integration option
This license provides the same functionality as Nozomi Networks Guardian IDS Integration option but the data is retrieved from existing Nozomi Networks Centralized Management Console. It is a sensor that manages mulitple Nozomi Guardians in a distributed environment.

Event Log Distribution Service (ELDS)
Event Log Distribution Service provides distribution of event information to external tracking systems:

- Windows Event Logo
- Syslog
- Email

Flexible rule-based notification profiles match items in the RUGGEDCOM CROSSBOW event log for distribution.

External Database Integration Service (EDIS)
External Database Integration Service shares device/gateway information with a secondary, external SQL database. During operation, RUGGEDCOM CROSSBOW polls the external database at user-specified intervals for new network-based devices and gateways.

File Export Service
File Export Service exports the files retrieved from end devices by RUGGEDCOM CROSSBOW to an external FTP/SFTP server.

SIEMENS

RUGGEDCOM CROSSBOW Starter Edition

Designed for smaller Industrial Control System (ICS) networks requiring secure password management to their remote site locations, RUGGEDCOM CROSSBOW Starter Edition provides for up to 5 users and 100 remote devices. As your network grows, optional CROSSBOW modules can be added for additional features and scalability.

CROSSBOW Starter Edition is an enterprise solution that provides cyber-secure local and remote user access for password management of remote devices. It allows an Intelligent Electronic Device (IED) maintenance application to remotely communicate with its associated IEDs as if the users were directly connected to the device. RUGGEDCOM CROSSBOW's client-server architecture is designed to allow an operator to easily manage remote connectivity to its entire population of field IEDs. User access is role based, and the user is not provided with any device password or network topology detail. All user activity is logged and reported per security best-practice recommendations.

RUGGEDCOM CROSSBOW Starter Edition

- One CROSSBOW Secure Access Manager server license
- 5 User licenses
- IED license for up to 100 devices
- User documentation

Ease of administration

- Administration interface allows management for remote IEDs and designated users
- Structured view of IEDs (region/site/gateway)
- Grouping of devices and users
- Configurable sub-admins

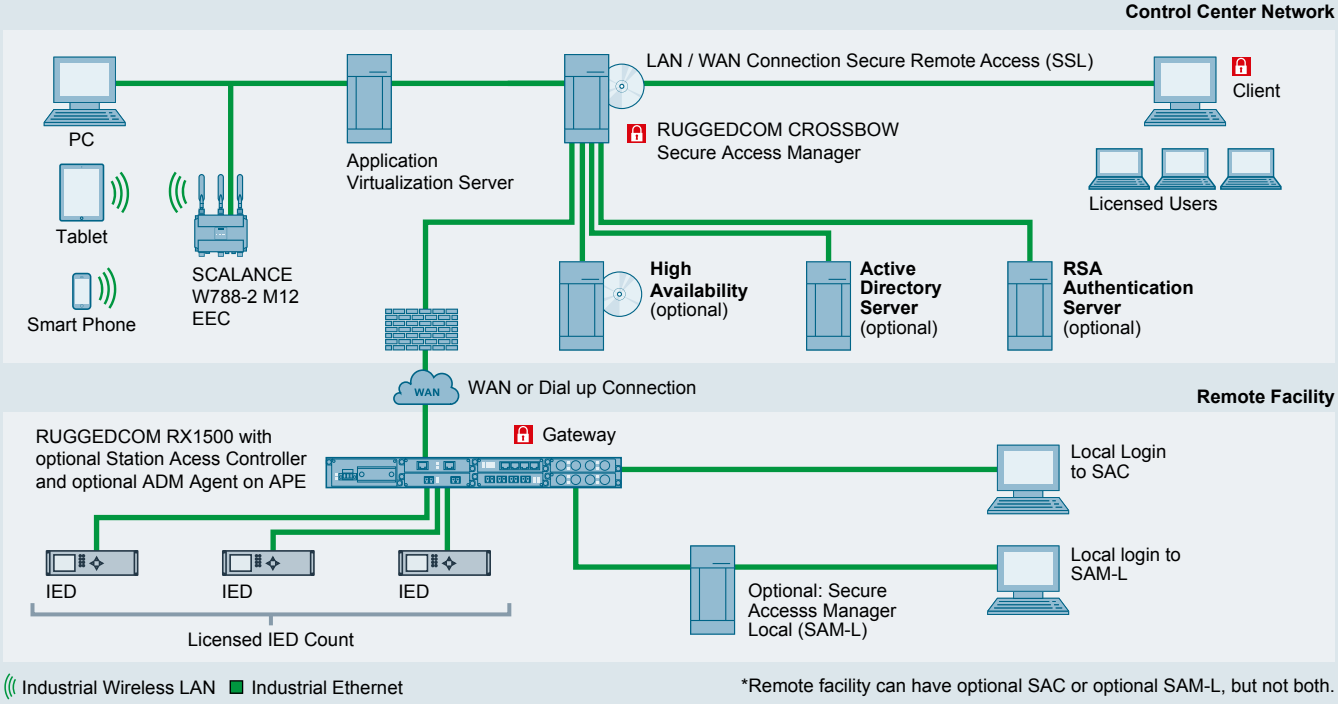
Flexible architecture

- Client-server or "clientless" architecture using virtual desktops
- Available redundancy
- Dial-up or WAN access

Broad device support

Preserves investment in legacy gateway devices and communication infrastructure

- RUGGEDCOM routers and switches
- Siemens SIPROTEC
- Garrettcom
- SEL
- GE
- ABB
- Cooper
- Many other IEDs



RUGGEDCOM CROSSBOW Secure Access Manager (SAM)

For user access to remote IEDs, the CROSSBOW clients establish secure SSL connections to the SAM. The SAM is connected via a secure WAN to gateway devices on the transformer substation, such as RUGGEDCOM RX1500 or another supported device. The gateway establishes the connection to IEDs either directly or through lower-level remote terminal units (RTU).

Typical workflow

RUGGEDCOM CROSSBOW is specifically designed to be intuitive and enhance users' normal activity. After logging in to the central SAM server, the user will be presented with a simple directory structure, displaying regions, facility sites, and devices, to which that user has been granted access to by the administrator. From there, the user simply clicks on a chosen device to display a list of applications associated with the device. Selecting a program will instruct RUGGEDCOM CROSSBOW to launch the application and initiate a connection to the device – no need to negotiate connections, boot applications, or remember passwords. In most cases – just one click – the user is interacting directly with the device. Sophisticated password management functionality allows remote management of router, gateway, and IED passwords supported. RUGGEDCOM CROSSBOW SAM also connects through to IEDs with their own direct modem access, such as for pole top applications, meters or process control, condition monitoring IEDs, and other host computer/servers. This ability of CROSSBOW to provide secure RBAC remote access to any IED makes it an essential tool for any IED-based application for electric, water and gas utilities.

Server and client requirements

RUGGEDCOM CROSSBOW is part of the Siemens family of communication products. It allows users to launch adevice maintenance application from a workstation located in a control center or at a facility and communicate with devices or gateways remotely as if the user were directly connected to the end device. Once connected, a user can maintain, configure, and/or retrieve information from the end device.

RUGGEDCOM CROSSBOW client-server architecture allows users to easily and securely manage remote connectivity to an entire set of field devices.

Please refer to the CROSSBOW Preparation Guide for the latest system requirements.

По вопросам продаж и поддержки обращайтесь:

Алматы (727)345-47-04
Ангарск (3955)60-70-56
Архангельск (8182)63-90-72
Астрахань (8512)99-46-04
Барнаул (3852)73-04-60
Белгород (4722)40-23-64
Благовещенск (4162)22-76-07
Брянск (4832)59-03-52
Владивосток (423)249-28-31
Владикавказ (8672)28-90-48
Владимир (4922)49-43-18
Волгоград (844)278-03-48
Вологда (8172)26-41-59
Воронеж (473)204-51-73
Екатеринбург (343)384-55-89
Иваново (4932)77-34-06
Ижевск (3412)26-03-58
Иркутск (395)279-98-46
Казань (843)206-01-48
Калининград (4012)72-03-81
Калуга (4842)92-23-67
Кемерово (3842)65-04-62
Киров (8332)68-02-04
Коломна (4966)23-41-49
Кострома (4942)77-07-48
Краснодар (861)203-40-90
Красноярск (391)204-63-61
Курск (4712)77-13-04
Курган (3522)50-90-47
Липецк (4742)52-20-81
Магнитогорск (3519)55-03-13
Москва (495)268-04-70
Мурманск (8152)59-64-93
Набережные Челны (8552)20-53-41
Нижний Новгород (831)429-08-12
Новокузнецк (3843)20-46-81
Ноябрьск (3496)41-32-12
Новосибирск (383)227-86-73
Омск (3812)21-46-40
Орел (4862)44-53-42
Оренбург (3532)37-68-04
Пенза (8412)22-31-16
Петрозаводск (8142)55-98-37
Псков (8112)59-10-37
Пермь (342)205-81-47
Ростов-на-Дону (863)308-18-15
Рязань (4912)46-61-64
Самара (846)206-03-16
Санкт-Петербург (812)309-46-40
Саратов (845)249-38-78
Севастополь (8692)22-31-93
Саранск (8342)22-96-24
Симферополь (3652)67-13-56
Смоленск (4812)29-41-54
Сочи (862)225-72-31
Ставрополь (8652)20-65-13
Сургут (3462)77-98-35
Сыктывкар (8212)25-95-17
Тамбов (4752)50-40-97
Тверь (4822)63-31-35
Тольятти (8482)63-91-07
Томск (3822)98-41-53
Тула (4872)33-79-87
Тюмень (3452)66-21-18
Ульяновск (8422)24-23-59
Улан-Удэ (3012)59-97-51
Уфа (347)229-48-12
Хабаровск (4212)92-98-04
Чебоксары (8352)28-53-07
Челябинск (351)202-03-61
Череповец (8202)49-02-64
Чита (3022)38-34-83
Якутск (4112)23-90-97
Ярославль (4852)69-52-93

Россия +7(495)268-04-70
Казахстан +7(727)345-47-04
Беларусь +(375)257-127-884
Узбекистан +998(71)205-18-59
Киргизия +996(312)96-26-47

эл.почта: rmi@nt-rt.ru || сайт: https://ruggedcom.nt-rt.ru/