VTScada Application Security

Standard Component

More Control, Less Complexity

All the security features in the world are of no use if they are so burdensome that operators and developers avoid using them. Like all our core SCADA features, we strive to make security management in VTScada simple and scalable, while remaining infinitely configurable. Security is managed within the standard operator interface, allowing authorized users to make changes without switching views; then instantly deploy those changes across the entire system without restarting.

Note: VTScada does not utilize Java and is therefore unaffected by Java-based exploits.

Integrated tools to support your security strategy

Centralized account management

Industry-standard encryption (TLS)

Read Only Server Options

Windows active directory support

Immediate application wide change deployment

OpenID Connect® for single sign-in and Two-Factor Thin Client authentication

Supports OAuth 2.0 for SMTP and POP3 authentication

Configuration traceability

Card-reader support

Implementations compliant with…

NERC/CIP (North American Electric Reliability Corporation)

DFARS 252 (Defense Federal Acquisition Regulations Supplement)

NIST 800 (National Institute of Standards and Technology)

Marine reliability standards ABS, Lloyds Bureau, DNV, BV

Options for Easy Login

Windows® Security Integration - Log on to VTScada using your Windows account. No need to manage both Windows and VTScada accounts.

Proximity Card Readers - Log on the same way you enter a secured building. Configure Operator Notes to require authentication.

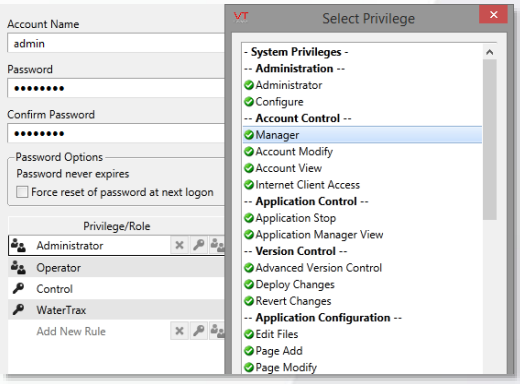
OpenID Connect® - Provides sign-in and Two-Factor Thin Client authentication.

A Smarter Approach to Account Management

Each application includes security accounts and settings that control access to the entire application including workstations, Internet clients, mobile Internet clients, and the VTScada Alarm Notification System. Authorized users can easily add, delete, copy, and modify accounts. Rather than making you choose from an ever-growing list of account privileges, VTScada uses 'Rules' and 'Roles'. The combination of the two allows you to generate highly-specialized user accounts in no time.

Rules - A combination of tags, privileges, and locations that allows you to finely tune what users can do and from where. This allows you to grant some users access to one part of a plant and others access to another part without creating any new privileges.

Roles - A set of Rules (and other Roles) corresponding to the duties of a specific job such as an operator at a specific plant.

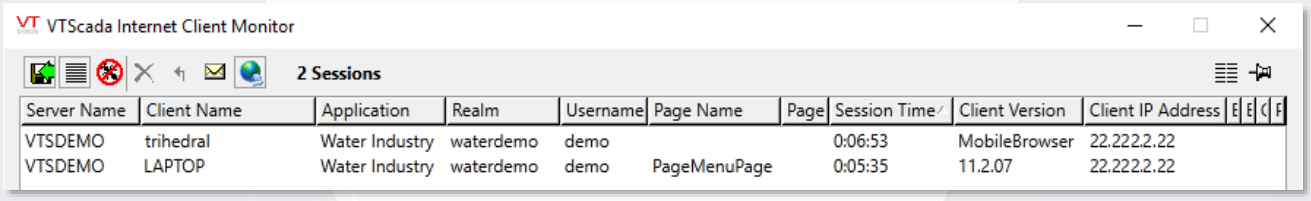


Unparalleled Traceability

Operations - Operator activity such as setpoint changes, logon/logoff, security modifications, and Alarm Roster activations are recorded as events by the VTScada Alarm Manager. This includes actions performed via servers, Thin Clients, and the VTScada Alarm Notification System.

Configuration - VTScada's built-in version control automatically tracks all changes made by all users on all workstations. It also detects manual changes to configuration files made by unauthorized users or malware, and automatically restores them to their correct state. The repository includes hash codes to detect any attempts to modify it. Authorized users can see this change history and instantly switch to any revision.

Remote Access - The VTScada Internet Client Monitor displays and logs VTScada Thin Client activity. Send messages to clients and force disconnection if malicious activity is suspected. Logs user IP, computer name, screens viewed, session length and other audit parameters.



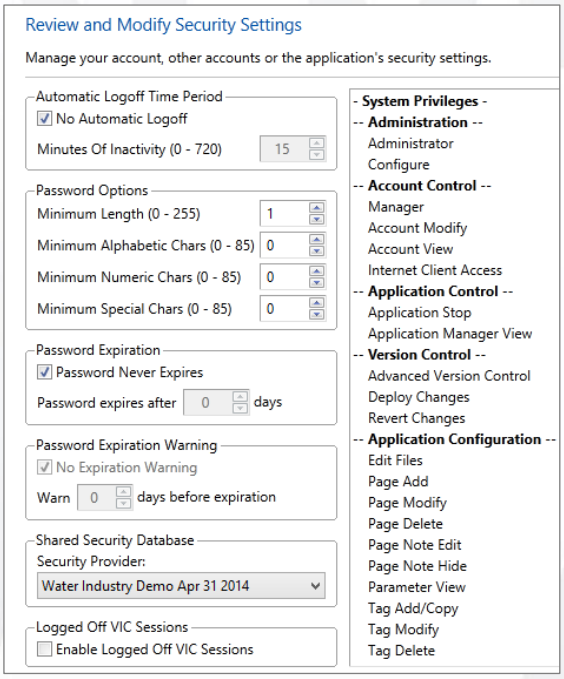
Server Name	Client Name	Application	Realm	Username	Page Name	Page	Session Time	Client Version	Client IP Address
VTSDEMO	trihedral	Water Industry	waterdemo	demo			0:06:53	MobileBrowser	22.222.2.22
VTSDEMO	LAPTOP	Water Industry	waterdemo	demo	PageMenuPage		0:05:35	11.2.07	22.222.2.22

Trihedral
A Delta Group Company

VTScada by Trihedral

Enhanced Password Protection

- Accounts can require passwords to exceed a minimum length, contain special characters, or expire after a defined period.
- Users can also be allowed to change their own passwords at will.
- Accounts can be disabled upon repeated failed log in attempts.



Enhanced Security with OpenID Connect®

- Permits integration of VTScada Security with third-party authentication servers on VTScada Anywhere Clients.
- Two-factor authentication (e.g., Google Authenticator or Apple Touch sensor) on VTScada Anywhere Clients.

Advanced Encryption and Network Protection

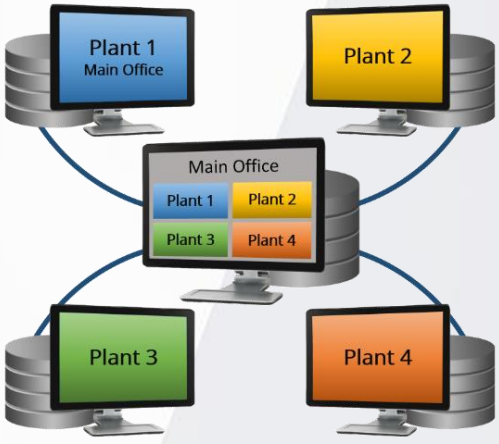
- Security database employs military-grade encryption as does the security information exchanged with Internet Clients.
- VTScada complies with industry-standard RFCs for security.
- User passwords are "hashed" meaning they are never held in a form that anyone can decrypt and recover.
- Time-stamped operator and trend notes are also encrypted to prevent deletion or modification.
- The VTScada Internet Client supports Transport Layer Security (TLS), firewalls, and VPN access.
- When emailing alarm notifications, VTScada now supports SMTP email servers requiring Transport Layer Security (e.g., Gmail®).
- Optionally configure a list of IP addresses that may or may not connect to your application.
- User-configurable IP port address and server failover methodology.
- If an unauthorized user attempts to modify a configuration file, the change will automatically be detected at startup and the current approved configuration file will be restored from the tamper-proof repository.

Secure Historical Data

- VTScada's historical file database cannot be edited within VTScada or by any third-party software tool. Not only are the proprietary log files not human readable, VTScada uses a checksum to detect any tampering or corruption.
- If you also log to a redundant third-party SQL format you will need to secure that database as per the manufacturer's instructions.

Large Systems Management Tools

- Define what information users can see in large applications.
- In a two-plant application, you can group the operators from each plant so that they can only see their own alarms and tags.
- Create another group for managers so they can see both plants.
- Master Applications allow you to centrally monitor tags, pages, alarms, and history from one or more independent sub-systems.



Download the 90-day Trial

Trihedral.com/trial

Updated December 14, 2021

VTScada.com
1.800.463.2783 (North America)
info@trihedral.com
1.902.835.1575 (Worldwide)
+44 (0) 1224 258910 (Europe)

Trihedral
A Delta Group Company