

VTS & VTScada Security Features

Application Security must be functional without being burdensome. Each VTS™ and VTScada™ application includes integrated security specific to that application. VTS uses privilege-based User Accounts to allow greater flexibility than security-level-based products. For simplicity, the same Accounts are used across all facets of the application, from logging into local workstations to VTS Internet Client and VTS Alarm Dialer access.

Summary

User Account Management Features

- Two-tier security access: Windows™ security for server, integrated security for application
- User-based accounts (each user has own account)
- Separate account management for each running VTS application
- Privilege-based accounts
- 35 default security privileges (i.e. Config, Admin, Alarm Acknowledge)
- Supports 64,000 custom privileges
- Supports privilege access to displays
- Supports privilege access to control functionality
- Area Filtering allows limited access to tags based upon User Accounts
- Privilege suppression
- User-changeable passwords
- All User Account changes are application-wide and immediate
- Add/copy/modify/delete User Accounts
- Automatic logoff timeout (adjustable)
- Minimum password length



Action Traceability Features

- Operator notes and trend notes include user's name
- Encrypted operator & trend notes storage
- Operational actions (i.e. logon/logoff, setpoint changes) saved to events log with user's name
- Configuration changes saved to events log with user's name

VTS Internet (Thin) Client Security Features

- Shares User Accounts with thick clients
- Specific account privilege to inhibit VTS Internet Client access to application
- Automatic logoff timeout applies
- Internet Client Monitoring tool tracks client activity and permits forcible disconnect
- Logging captures user IP, computer name, screen viewed, time plus many other audit parameters
- Supports SSL (Secure Socket Layer), firewalls & VPN access
- User configurable IP port address and server failover methodology
- Ability to sub-divide access into assigned Realms limiting user application access
- Does not require the use of Microsoft IIS™ or third-party web server
- Users are not required to be given Windows™ level security on server
- Authentication does not utilize MS DCOM™, thus maintaining firewall security

- **VTS Alarm Dialer Security Features**
- Shares User Accounts with thick clients
- Logon required for dial-In for status and dial-out for alarm acknowledgement

VTS WAP Server Security Features

- Shares User Accounts with thick clients

File Management Security Features

- Encrypted account information storage
- Edit/Lockout service manages synchronization of files across all servers and clients
- Binary formatted raw historical data minimizes tampering

Security Features Described

How Accounts are Used

User Accounts are specific to each application. This provides the flexibility to run multiple applications with differing security requirements on a single computer.

Each user for a particular VTS application is generally given a user account. This account not only provides access to the application, but also ensures activities within the system can be traced back to the user responsible.

Accounts may also be created for specific roles, such as 'Operator' or 'Guest'. Such accounts provide far less traceability, but facilitate access to applications where users frequently change (i.e. public access sites).

Accounts Management

Account Management is completed within the standard operator interface, allowing users with the proper privileges to make security changes without switching views.

All changes to security are immediate and system-wide, forcing all application machines, including Internet clients, to obey the new rules without delay. For example, new users can be added and process views can be secured without stopping and restarting VTS clients or servers.

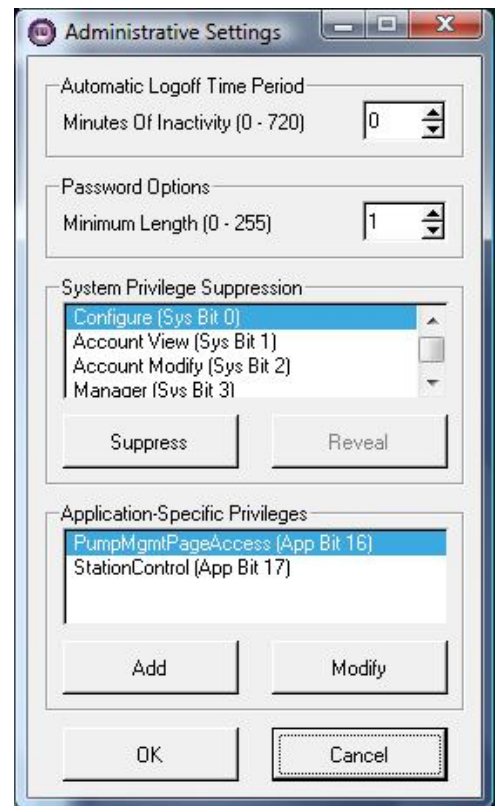
Administrators may set system-wide automatic timeouts on accounts, forcing idle accounts to be automatically logged out of the application. This feature both minimizes the likelihood of malicious activities on unattended workstations and ensures concurrent Internet client connections are not unintentionally held indefinitely when not in use. Users may be permitted to set their own passwords; however, administrators can create a minimum password length requirement.

Accounts can be added, deleted, modified and copied. Copied accounts can then be customized by adding or removing privileges. For example, a typical operator account may be created as a template and then copied and customized to meet the needs of each additional operator.

Account Privileges

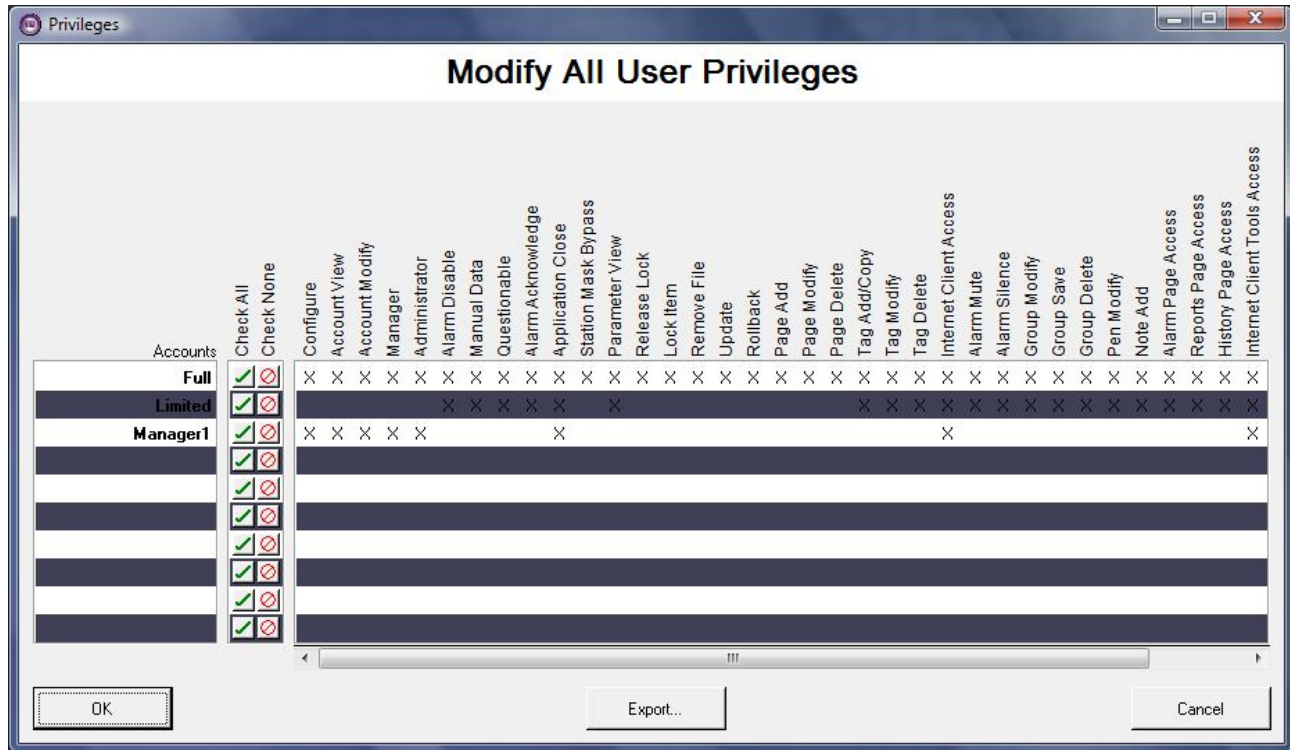
User Accounts are privilege-based, rather than security level based. There are 35 default privileges, as shown in the screen shot on the next page, and an additional 64000 custom privileges may be added to limit access to display pages and control functionality.

In the event a specific privilege is not considered appropriate for a particular application, the privileges may be suppressed. Suppressed privileges cannot be given to any account and are not displayed on user account privilege management display.



Area Filtering by Account

Applications can be configured to allow access to specific functional areas based upon each user's account. For example, a single application may have two functional areas, such as Water Plant 1 and Water Plant 2. (See image below) When a user from Water Plant 1 logs into the application, they see data from that area, whereas a user from Water Plant 2 can log into the same application on the same computer and see Water Plant 2. Similarly, a manager or system administrator account may be configured to see both areas.



Traceability of Actions

Operational and configuration user actions are saved in chronological order to the VTS Event History. Such actions include logon/logoff, security modifications and control actions. This functionality extends to actions performed by users connected via thick clients, VTS Internet Clients, the VTS Alarm Dialer or via WAP enabled devices.

Operator notes, added to a set of trended values or to the Operator Notes Log, include both a timestamp and the user's account name. The notes log is encrypted and does not allow editing of existing notes, ensuring the notes log cannot be altered.

Internet (Thin) Client Security

Internet connectivity security is managed as a property of the standard VTS User Account and is therefore managed from the standard security manager interface. As with other security privileges, Internet access can be granted or revoked from any user account and the changes are applied immediately and system wide.

VTS Internet Client licenses are concurrent, in that a user logging onto the application has exclusive use of one VTS Internet Client license for the duration of the connection and that license will be returned to the pool when the connection has terminated.

It is therefore important to ensure that connections to the application can be terminated to return licenses to the pool as necessary, or in the event malicious activity is suspected. The account timeout option, as described above, extends to Internet client connectivity, ensuring users cannot leave account connections open indefinitely. Additionally, the VTS Internet Client Monitoring tool can be used to monitor and log client activity, send messages to clients, and force disconnection of any user connected via a VTS Internet Client.

The tool (shown below) collects the name and IP of connected computers as well the application name, page viewed and the user name of the account being used to access the application.

Access to applications can be further restricted by creating a list of allowed or disallowed IP addresses, though such limitations are not recommended for applications where users require access from public computers or use computers with dynamic IPs.

Alarm Dialer Security

The VTS Alarm Dialer supports alarm dissemination via email, alphanumeric pager and text-to-speech over telephone dial-out. Users contacted by a VTS application over dial-out must enter a valid password using the dial-pad keys before alarms can be acknowledged. This is the account password used to connect to the application from thick and thin clients.

Dial-in access requires the same password. Once the password has been validated by VTS, users may listen to status information (i.e. temperature, flow, etc) and may acknowledge alarms.

WAP (Wireless Application Protocol) Security

Devices such as Blackberry PDAs and some cellular phones support wireless application connectivity via WAP. The optional VTS WAP Server product allows such devices to access VTS or VTScada applications. Users are then able to view status information, perform control actions and acknowledge alarms from anywhere they can use their cellular phones. Standard VTS User Account privileges apply to all WAP access.

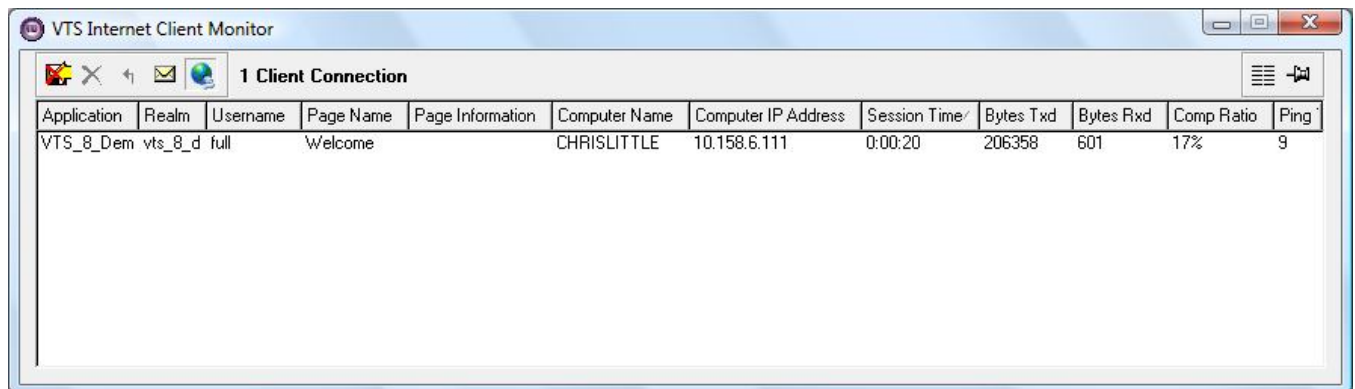
File Management Security

To ensure security account information cannot be accessed by unauthorized users, security account information is saved in an encrypted file. Within the security interface, passwords are displayed using the * symbol.

By design, there is no method by which raw VTS historical log files can be edited. Such files are maintained in binary format to minimize tampering. Where editing of logged data is required, data should be exported to a separate location where editing does not effect the integrity of the raw files.

VTS file management is handled on a system-wide basis to ensure each server is updated with an identical set of application files. The integrated VTS Edit/Lockout Manager identifies one server which will be responsible for this task, such that in the event file corruption or tampering has occurred, servers and clients can easily be realigned with the primary server.

In addition to the embedded VTS Internet security features, VTS integrates with industry-standard Internet security features, such as SSL (Secure Socket Layer), firewalls, and VPN access.



Contact Trihedral

1.800.463.2783 (toll-free) sales@trihedral.com

www.trihedral.com