Security Best Practice for Trend Products

IMPORTANT

Strong cyber security results from a partnership between manufacturers, system integrators, and end-users.

Security for sites has to be evaluated on a case-by-case basis, but Trend strongly advises systems are not directly accessible from the internet, and the systems are placed on a secured network. If possible, utilising vLANs and VPNs.

As a minimum Trend recommends systems are regularly reviewed to ensure the system is updated to the latest version for each component part and configured with strong usernames and passwords.

- **Ensure any of the products security features are not bypassed, and individual user accounts are used with strong passwords.**
- **Never connect Trend IP based products directly to the internet. If remote connectivity is required use a VPN.**
- **Ensure physical access to the network and control devices is restricted to authorised personnel only.**

While it is impossible to make any system completely impenetrable, there are many ways to build up a system that is more resistant to attacks or modifications to operational parameters as a result of weak system configuration. This document describes how you can help make a Trend system more secure with careful configuration.

Note: Restricting physical access to the networks, controllers, displays and PC running Trend software is as critical to security as the software settings outlined in this document.

If in any doubt consult your IT support/manager/business partner or other IT security professional.

CONTENTS

1. Why Secure Your BEMs? 1
2. Security Design Principles 2
3. System Security Overview 3
4. Mobile Device Security 3
5. SNMP Data Considerations 3
6. Personally-identifiable information 3
7. Secure data stores 3
8. Securing the Operating System 4
9. Restricting access to network & Storage media 4
10. Network isolation 4
11. Traffic type restriction 4
12. Secure WAN remote access 4
13. Internet Connection 4
14. Securing Strategy 5
15. Securing Web Servers 5
16. Securing email Destinations 5
17. Application/Firmware Version 5
18. Users & Passwords 5
19. Securing the Plant Systems 6
20. Trend Niagara based products 6
21. Trend Products Using SQL Server 7
22. Trend Energy Manager 8
23. Limitation of Liability 8

1. WHY SECURE YOUR BEMS?

- Protect your customer's plant systems from unauthorised changes to operating set-points, overrides and time schedules.
- Prevent access to user account details: e.g. usernames, passwords, email addresses, SMS (mobile) numbers etc.
- Prevent access to commercially-sensitive data: e.g. energy consumption metrics, specialist control strategy solutions etc.
- Prevent unauthorised access to PC and networks hosting BEMS software and control devices.
- Maintain data integrity and provide full auditing and accountability.

2. SECURITY DESIGN PRINCIPLES

System engineers should always follow the principle of 'least privileges' when configuring or modifying the Trend BEMS. I.e. only granting access to the minimum set of elements needed for a client to perform their job and ensuring each individual has their own login account.

The following security design principles should be considered:

- **Least Privilege**
  The Least Privilege design principle requires any user is only given the necessary minimum level of access for the minimum amount of time.

  E.g. When configuring users for a supervisor each user should be given the minimum level of access required to carry out the necessary tasks, and timeouts should be set for the users.

- **Fail-Safe Defaults**
  The Fail-Safe Defaults design principle ensures that when there is a failure the system confidentiality, integrity and availability is maintained.

  E.g. If a controller is compromised and set to turn the heater battery on without the fan, then hardware interlocks should prevent it happening.

- **Economy of Mechanism**
  The Economy of mechanism design principle requires that systems should be kept as simple as possible. The likelihood of vulnerabilities and errors increases with the complexity of design.

- **Psychological Acceptability**
  The Psychological Acceptability design principle refers to security mechanisms not making resources more difficult to access than if the security mechanisms were not present. If you make things too difficult for users they are likely to make things less secure.

  E.g. While you need to comply with good password rules and selection, do not create a password policy that makes it too difficult for users to remember their passwords or make the process too onerous as this will make users more likely to write passwords down.

  Note: Remember that if passwords are difficult to remember a password manager could be used.

- **Defence in Depth**
  The Defence in Depth design principle is a concept of multiple layers of controls and risk-mitigation countermeasures are incorporated so that there is no single point of complete compromise.

  E.g. For a supervisor there could be 4 levels of defence:

  - PC in access controlled location
  - Log on required to PC
  - Log on required to supervisor application
  - Level of access to application need to allow required change

  Or for a controller there could be 4 levels of defence:

  - Controller in locked cabinet
  - Physical access to network cabling restricted
  - vLAN used for Ethernet network
  - Users configured in controller

  If any one of these controls is breached, then the system can still remain secure.

3. SYSTEM SECURITY OVERVIEW

The diagram below shows the different levels of a BEMS system and what assets / protection should be considered at each level.

System Level		Considerations
Mobile	Operating System	Operating system version - see **Operating System Version**.
	Hardware (e.g. mobile phone)	Secure device against unauthorised access - see **Mobile Device Security**.
Supervisors Tools Displays	Internet Services	Web server must use HTTPS with trusted certificate - see **Securing Web Servers**. Use secure email providers - see **Securing email Destinations**. SNMP data content - see **SNMP Data Considerations**.
	Application (e.g. IQ®VISION)	Application version - see **Application/Firmware Version**. Users and passwords - see **Users & Passwords**. Personally-identifiable information - see **Personally-identifiable information**. Secure data stores - see **Secure data stores**.
	Operating System	Follow general best practice - see **General Good Practice**. Firewall settings - see **Firewall settings**. Operating system version - see **Operating System Version**. Virus protection - see **Virus Protection**. Intrusion protection - see **Intrusion Protection**. Users and passwords - see **Users & Passwords**.
	Hardware (e.g. PC)	Restriction of physical access - see **Restriction of Physical Access**.
Gateways		Restriction access to network media - see **Restricting access to network & Storage media**. Network isolation - see **Network isolation**. Traffic type restriction - see **Traffic type restriction**. Secure WAN remote access - see **Secure WAN remote access**.
Controllers/Displays		Firmware version - see **Application/Firmware Version**. Restriction access to network and storage media - see **Restricting access to network & Storage media**. Network isolation - see **Network isolation**. Users and passwords - **Users & Passwords**. Web server must use HTTPS with trusted certificate - see **Securing Web Servers**. Secure WAN remote access - see **Internet Connection**. Secure email providers - see **Securing email Destinations**.
Control Strategy		PIN levels set for ALL adjustments - see **PIN levels set for ALL adjustments**. Top and bottom ranges set - see **Top and bottom ranges set**.
Plant Systems		Hardware interlocks - **Securing the Plant Systems**.

4. MOBILE DEVICE SECURITY

The mobile device must be secured against unauthorised access e.g. PIN, password or fingerprint access must be enabled.

5. SNMP DATA CONSIDERATIONS

SNMP is inherently insecure therefore its use should be avoided where possible. If it is to be used be aware of personally identifiable information that could be being transmitted.

6. PERSONALLY-IDENTIFIABLE INFORMATION

When configuring the system consider the consequences of sensitive data falling into the wrong hands. E.g. labels that identify location etc. Any use of such information must comply with all applicable data protection regulations.

7. SECURE DATA STORES

The underlying data store (e.g. SQL) **MUST** be secured according to the manufacturer's recommendations. Some Trend products use SQL see **Trend Products Using SQL Server**.

8. SECURING THE OPERATING SYSTEM

8.1. GENERAL GOOD PRACTICE

Follow general good practice for securing the operating system such as:

- Password protected screen saver
- Drive encryption software

8.2. FIREWALL SETTINGS

The operating system must be configured to use a firewall which is automatically updated. The configuration must prevent access (IN/OUT) for all ports except those for which access is required, **DO NOT** leave any unused ports open.

8.3. OPERATING SYSTEM VERSION

You **MUST** ensure that any device running Trend applications or connected to the same IP network has the latest operating system updates installed. It is good practice to ensure that Windows Updates are left on automatic and that they are installed in a timely manner.

8.4. VIRUS PROTECTION

You **MUST** ensure that any PCs running Trend applications or connected to the same IP network are running virus protection software, and the virus definitions are kept up-to-date.

8.5. INTRUSION PROTECTION

The use of an Intrusion Detection System (IDS) from a reputable provider of security products on any PC running a Trend application is recommended. Follow best practice for the products chosen as well as any corporate IT policy where the installation is made.

Many IDS and firewall products offer a complete solution for recording all the traffic coming in and out of the PC, providing users with the ability to record all activity at the lowest level.

8.6. RESTRICTION OF PHYSICAL ACCESS

The device running the application **MUST** be secured against unauthorised physical access. Any network cabling **MUST** also be secured against physical access.

9. RESTRICTING ACCESS TO NETWORK & STORAGE MEDIA

Prevent unauthorised access to the storage media (e.g. SD card) and network media (e.g. Ethernet/Trend LAN, BACnet) that is used by the supervisor/tool/controller/display. With any system, preventing physical access to the network and equipment reduces the risk of unauthorised interference. Trend Control equipment should be installed within locked control cabinets, themselves located in secured plant rooms.

10. NETWORK ISOLATION

- **Configure separate IT networks for the BEMS and the customer's corporate IT Network.**
  This may be achieved by configuring vLAN's (Virtual LAN's) within the customer's IT infrastructure or by installing an air-gapped separate network infrastructure dedicated to the BEMS.

- **Use Dynamic vLANs with MAC address allocation**
  This can protect against the unauthorised connection of a device into the system and can reduce the risk associated with an individual monitoring information on the network.

11. TRAFFIC TYPE RESTRICTION

Once the system has been commissioned, restrict IP traffic on the BEMS IT network (for example using access lists) to the types of protocols required for normal operation, i.e. Supervisor vCNC, alarm delivery and Trend network map traffic. Further information regarding the communications traffic required for normal operation can be found in the product documentation.

When interfacing with the Trend system using a centralised system supervisor (e.g. IQ®VISION) and where the system does not require direct access to the individual devices web server, web server should be disabled and/or the network infrastructure should be configured to restrict web server access.

12. SECURE WAN REMOTE ACCESS

If remote access is required into the Trend system, use VPN (Virtual Private Network) technology to reduce the risk of data interception and protect the controls devices from being directly placed on the internet. For more details and an example configuration please refer to the 'Using a VPN with Trend Systems' guidance document.

13. INTERNET CONNECTION

IQ controllers **MUST** never be directly connected to the internet in any form. Use of 'hidden' ports or any other form of trying to 'hide' the system is **NOT** a solution. If remote connection is required, use a VPN.

14. SECURING STRATEGY

In addition to the points below the strategy must be configured with users, passwords and PINs - see **Users & Passwords**.

14.1. PIN LEVELS SET FOR ALL ADJUSTMENTS

Appropriate PIN levels must be set for all adjustments within the strategy to prevent unauthorised changes.

14.2. TOP AND BOTTOM RANGES SET

The top and bottom range for all knob modules must be set to ensure the value cannot be adjusted outside the expected range.

15. SECURING WEB SERVERS

If the product's web server is to be used it **MUST** be configured to use HTTPS with a trusted certificate. If the web server is not required it **MUST** be disabled.

16. SECURING EMAIL DESTINATIONS

If the product supports the sending/receiving of emails a secure email provider **MUST** be used.

17. APPLICATION/FIRMWARE VERSION

Trend regularly updates the applications and firmware to add additional features and improve system security. You **MUST** ensure that the latest version is used and it is kept up-to-date with latest version.

18. USERS & PASSWORDS

18.1. USERS

Ensure the number of users and access levels provided are appropriate for the activities they need to perform.

- **At the controller device level configure users in controllers for Web client, Supervisor and Peer-to-peer access.** Configuring User modules in the IQ® controllers, this means a user will have to log into a device with valid credentials before adjustments can be made. Ensure appropriate user levels are assigned for the site users, from an administrator user (Level 99), through general user (Level 1 to <70) to Guest user. Please see the appropriate IQ® configuration manual for specific details on configuring users.

  Controllers have a default user 'System Guest' which exists in all controllers. When a user accesses the controller via its web page they will be given the access rights of the System Guest and a user level of 100 (total access).

  It is therefore necessary to configure a 'Guest' user which determines the access given to users without passwords, this user should be configured with the minimum access.

- **Use a Different Account for Each User**
  Use unique user names and passwords for each user of the system, rather than generic user access. Different people should never share the same account. For example, rather than a general 'managers' user that many managers could use, each manager should have their own, separate account.

  There are many reasons for each user to have their own individual account:

  - If each user has their own account, audit logs will be more informative. It will be easy to determine exactly which user did what. This can help detect if an account has been compromised.

    Note: Not all products have an audit log facility, but where available is should not be disabled.

  - If a user account is removed or modified, it does not inconvenience many users. For example, if a user should no longer have access, deleting their individual access is simple. If it is a shared account, the only options are to change the password and notify all users, or to delete the account and notify all users. Leaving the account as-is is not an option – the goal is to revoke the user's access.
  - If each user has their own account, it is much easier to tailor permissions to precisely meet their needs. A shared account could result in users having more permissions than they should.
  - A shared account means a shared password. It is an extremely bad security practice to share passwords. It makes it much more likely for the password to be leaked, and makes it more difficult to implement certain password best practices, such as password expiration.

- **Use Unique Engineering Users for Projects**
  It is a common practice that some companies use the same user details on every project. Once this is known if one system is compromised, the attacker could potentially have credentials for access to many other projects installed by the same company.

- **Disable Known Accounts When Possible**
  Some products have default accounts. These should be configured so that the password is no longer the default.

- **Assign the Minimum Required Permissions for users**
  Ensure only required users are set up on the system with the minimum security levels required rather than full access. When creating a new user, think about what the user needs to do in the system, and then assign the minimum permissions required to do that job. For example, a user who only needs to see alarms does not need access to the controller Configuration mode in 963. Giving permissions which are not required increases the chance of a security breach. The user might inadvertently (or purposefully) change settings that they should not change.

- **Use Minimum Possible Number of System Administrator account**
  Only assign System Administrators permissions when absolutely necessary. This type of account is an extremely powerful account – it allows complete access to everything. Only the system administrator should have access to the account. Also think about providing the System Administrator two accounts, one for daily access to manage day to day activities, and a second high level access account which is only required when administration type changes are required.

18.2. PASSWORDS

The Trend system and operating systems used Trend products use passwords to authenticate 'users' into a Supervisor, Display, Tool or Operating systems. It is particularly important to handle passwords correctly. Not employing this most initial level of security will mean anyone accessing the system via a display, web client or supervisor will have access to make adjustments. Ensure the Trend system operates an appropriate password policy for user access this guideline would include, but not limited to:

- **The use of strong passwords**
  Not all passwords are equally effective. Ensuring that users are choosing good, strong passwords is essential to securing a system. A single word, followed by a number (for example, "password1), or a birthday (for example, "May151970) may be easy to remember, but it is also easy for an attacker to guess. A random string of characters (for example, "s13pj96t!cd"), or a few words strung together in a nonsensical sentence (such as, "StrangeCoffeeRabit") are much stronger and more difficult to guess. However also remember the psychological acceptability of these requirements and try to design your system to be both easy to use, as well as secure.
- **A recommended password cycle time**
  Some Trend products allow the system administrator to specify a period after which a user must change their password. Although not all products currently enforce this password change period a site policy can recommend this to users.
- **Password disclosure rules**
  The user **MUST** ensure that they do not disclose details of their user name and password, to others and to not write them down.

19. SECURING THE PLANT SYSTEMS

Hardware interlocks should be installed to prevent damage in the event of incorrect system configuration.

20. TREND NIAGARA BASED PRODUCTS

For Trend products which are based on the Niagara N4 and Niagara AX frameworks (e.g. IQVISION, TONN, TOPS), you must follow Tridium's advice on securing the Niagara framework.

There are a number of configuration changes that can be made to Niagara that can be done to maximise the security of Trend products.

- Use the Password Strength Feature
- Enable the Account Lockout Feature
- Expire Passwords
- Use the Password History
- Use the Password Reset Feature
- Leave the "Remember These Credentials" Box Unchecked
- Change the Default System Passphrase
- Use TLS To Set the System Passphrase
- Choose a Strong System Passphrase
- Protect the System Passphrase
- Ensure Platform Owner Knows the System Passphrase
- Use a Different Account for Each Platform User
- Use Unique Account Names for Each Project
- Ensure Platform Owner Knows the Platform Credentials
- Use a Different Account for Each Station User
- Use Unique Service Type Accounts for Each Project
- Disable Known Accounts When Possible
- Set Up Temporary Accounts to Expire Automatically
- Change System Type Account Credentials
- Disallow Concurrent Sessions When Appropriate
- Configure Roles with Minimum Required Permissions
- Assign Minimum Required Roles to Users
- Use the Minimum Possible Number of Super Users
- Require Super User Permissions for Program Objects
- Use the Minimum Required Permissions for External Accounts
- Use an Authentication Scheme Appropriate for the Account Type
- Remove Unnecessary Authentication Schemes
- TLS & Certificate Management
- Module Installation
- Require Signed Program Objects and Robots
- Disable SSH and SFTP

- Disable Unnecessary Services
- Configure Necessary Services Securely
- Update Niagara 4 to the Latest Release
- Install Product in a Secure Location
- Make Sure that Stations Are Behind a VPN

Specific technical publications are available which must be followed to ensure the system is locked down as securely as possible. Many options exist such as SSL encryption and additional steps to protect elements such as program modules, for more details refer to the Tridium website for the Niagara 4 Hardening Guide (for Niagara N4 based products) and the Niagara Hardening Guide (Niagara AX based products).

21. TREND PRODUCTS USING SQL SERVER

For all Trend products that use SQL server you must follow Microsoft's advice on securing SQL Server. There are a number of configuration changes that can be made to SQL Server that can be done to maximise the security of Trend products.

- Run SQL Server in Windows Authentication Mode
- Run SQL Server Under a Specific Windows User Account
- SQL and Windows User Logins
- Disable Remote Connection to SQL Server
- Restrict SQL Servers Ability to Perform Command Execution
- Review the SQL 'Sa' User's Password
- Review SQL Users
- Ensure SQL Server is Up-to-date

For general operation the user does not need to know the login details associated with SQL server, the SQL server access is only for the Trend product to interact with SQL server.

Note: The following guidelines assume the SQL server configuration on the machine is dedicated to Trend product and has been installed as part of the installation. It assumes there are no requirements for third-party network or local access to SQL server or the product's database.

21.1. RUN SQL SERVER IN WINDOWS AUTHENTICATION MODE

To secure SQL Server it is recommended to operate using 'Windows Authentication' and not 'SQL Server and Windows Authentication mode' (mixed mode). Mixed mode allows applications to log on to the SQL application using their own database user and password, Windows authentication mode only allows SQL to operate with the operating system privileges of the user account currently logged onto the PC.

Note: Trend Energy Manager is only able to access SQL Server in Mixed Authentication Mode. Trend Energy Manager runs in its own SQL instance with instance specific credentials. Therefore it is not possible to run SQL Server in Windows Authentication mode when using Trend Energy Manager.

Note: Any windows users that require to run 963 must be a member of the SQL server user's workgroup.

21.2. RUN SQL SERVER UNDER A SPECIFIC WINDOWS USER ACCOUNT

If the product is to only be used by a single Windows user and security is of high importance SQL server can be configured to run under a specific Windows user account. This will prevent other users of the PC from running SQL server and therefore the Trend product (e.g. 963).

Note: This user should be a user in the 'Power Users' workgroup, and must have read/write access rights to the location on the network to which backups are to be made.

21.3. SQL AND WINDOWS USER LOGINS

If SQL Server is configured to operate in 'Windows Authentication mode' only, any users that are to run the Trend product must have access to SQL server. If the user is an 'Administrator' user (is a member of the 'Administrator' workgroup) it will have access to SQL server and no additional configuration is necessary. However if the user is not is a member of the 'Administrator' workgroup it is necessary to give the user access to SQL server by making the user a member of the SQL server user workgroup.

21.4. DISABLE REMOTE CONNECTION TO SQL SERVER

If the SQL Server is dedicated to Trend product and no external interaction is required across the network then remote connections to SQL should be disabled.

Note: This does not prevent web clients from accessing the products web server data (if supported).

21.5. RESTRICT SQL SERVERS ABILITY TO PERFORM COMMAND EXECUTION

xp_cmdshell can allow programs with access to SQL the ability to issue operating system commands directly to the Windows command shell, for example create new databases or browse a network directory. The Trend products require this feature during installation and upgrades, but for a secure system it is recommended to disable this following installation.

Note: In this mode, older versions of 963 will display warning messages when starting up under normal conditions (i.e. not upgrading). These can be safely ignored.

21.6. CHANGE THE SQL SERVER'S SYSTEM ADMINISTRATOR USER'S PASSWORD

When SQL Server is installed with a Trend product, the Trend product generates an SQL account which is the SQL Servers system administrator account. To ensure security this password MUST be reviewed and if necessary changed to ensure security.

Important: A record of the SQL administrator password must be kept in a safe place (e.g. a firesafe) or in a password manager like LastPass.

21.7. REVIEW SQL USERS

During the installation of SQL by a Trend product a system administrator user is created. Some Trend products will create other users (e.g. 963 creates a SQL user called 'i96X1'). Other SQL users or user groups can be deleted, providing they are not required by other applications and deletion is allowed by SQL. The system administrator user must not be deleted.

21.8. ENSURE SQL SERVER IS UP-TO-DATE

It is important to regularly update SQL Server with all hot fixes, and service packs as recommended by Microsoft®. The 'Microsoft Baseline Security Analyser' is a utility that scans for common insecurities in configuration and make recommendations. It can check if SQL server 2008 is patched to the latest version, but currently does not check for configuration vulnerabilities, however SQL Server 2008 Best Practice Analyser can provide this functionality. The operation of this tool should be included in regular administration tasks with the SQL server system.

22. TREND ENERGY MANAGER

Organisations running the Trend Energy Manager (TEM) software on premise are strongly advised to restrict access to the product's web portal to users within their organisations internal network (Intranet). If external access is necessary then a VPN must be used in addition to the general guidance within this information sheet.

23. LIMITATION OF LIABILITY

Trend & Honeywell's liability in respect of any purchase order, any cyber security event or otherwise under trading terms and conditions shall in no case exceed the contract price of the specific Goods that give rise to the claim.

The installer shall operate a fully documented policy which as a minimum complies with the requirement detailed in this document

- The policy should demonstrate that the installer considers Cyber Security as a significant issue and the potential impact on the BEMS is clearly communicated to all its Customers.
- If the installer is aware of any BEMS Systems using Trend products which it has installed and is unsecure then the installer shall take proactive steps to inform its Customer putting forward recommendations to minimise any likelihood of a security breach.

The installer acknowledges and agrees:

- Installer is responsible for providing and maintaining and operating environment with at least the minimum standard specified by Trend. This includes complying with applicable Cyber security standards and IT security best practices including those recommended by any National Institutions in the Customers territory.
- To promptly notify Trend if a Cyber security event occurs and facilitate Trend's investigation of any cyber security event involving the Goods, Software or Services, installer will cooperate with Trend in any investigation, litigation or other action, as deemed necessary by Trend to protect its rights relating to a Cyber Security event.
- If a Cyber Security event occurs installer shall take reasonable steps to immediately remedy any event and prevent further events at installer expense in accordance with applicable laws regulations and standards. Installer further agrees that it will use its best efforts to preserve forensic data and evidence in its response to a cyber security event. Installer if requested will make available this forensic evidence and data to Trend.
- Trend shall not be liable for damages caused by a Cyber Security event resulting from Installers failure to comply with these terms or Installers failure to maintain reasonable and appropriate security measures.

Please send any comments about this or any other Trend technical publication to techpubs@trendcontrols.com

Trend Control Systems Limited

Albery House, Springfield Road, Horsham, West Sussex, RH12 2PQ, UK. Tel:+44 (0)1403 211888 Fax:+44 (0)1403 241608 www.trendcontrols.com