These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: Dec 2019
Issued: May 2013


* Indicates a trademark of General Electric Company and/or its subsidiaries. All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation. Please send comments or suggestions to controls.doc@ge.com

Public Information
## Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Custom Network Switch Layout Configuration</td>
<td>Added Monitoring properties to the Network Switch Layout Configuration Properties table</td>
</tr>
<tr>
<td></td>
<td>Switch Stacking and Hardware Monitoring</td>
<td>New section</td>
</tr>
<tr>
<td>N</td>
<td>Trunk Port</td>
<td>Updated the first paragraph with trunk port description and use</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>New sections to describe new port connection types</td>
</tr>
<tr>
<td></td>
<td>Thin Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Temporary Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Switch Layout Overview and Configuration</td>
<td>Updated to provide overview, configuration details for new sites, upgrade instructions for existing sites, support for newly qualified NetworkST standard switch types, and custom configuration</td>
</tr>
<tr>
<td>M</td>
<td>Configure Network Switch Configurations to Use Management Network</td>
<td>Update screenshot to include the Switch Layout Type property and added the table Network Switch Configuration Properties</td>
</tr>
<tr>
<td></td>
<td>Network Switch Layout Configuration</td>
<td>New section</td>
</tr>
<tr>
<td></td>
<td>Thin Client HMI Support</td>
<td>Moved to this document from Workstation Network Monitor Instruction Guide (GEI-100693) as the Thin Client can only be configured from CSH</td>
</tr>
<tr>
<td></td>
<td>Troubleshoot Network Switch SNMP Issues</td>
<td>Moved from Appendices to body of the document, and renumbered remaining Appendices</td>
</tr>
<tr>
<td>L</td>
<td>Thin Client Configuration Properties</td>
<td>Updated the description for DHCP Enabled in the Configuration Properties table</td>
</tr>
<tr>
<td></td>
<td>Configure Network Settings</td>
<td>Updated to include a description and the procedures to enable and disable the DHCP Enabled network settings</td>
</tr>
<tr>
<td>K</td>
<td>Overview</td>
<td>Added remote desktop connection monitoring to the bullet item regarding Computer Health group functionality</td>
</tr>
<tr>
<td></td>
<td>Data Flow</td>
<td>Added remote desktop connection to the bullet item regarding Computer Health, and added a bullet item for Control Server health monitoring</td>
</tr>
<tr>
<td></td>
<td>Remote Desktop Protocol (RDP) Connections Threshold Alarm</td>
<td>New section describing the RDP Connections Threshold Alarm feature</td>
</tr>
<tr>
<td></td>
<td>WorkstationST Computer Health Information</td>
<td>Updated the procedure steps and the graphic</td>
</tr>
<tr>
<td>J</td>
<td>Overview</td>
<td>Added a reference to the ToolboxST User Guide for Mark Controls Platform (GEH-6700 or GEH-6703) for a list of recommended and supported OS</td>
</tr>
<tr>
<td></td>
<td>Network Switch SNMP Configuration</td>
<td>New chapter added to distinguish SNMP V1 and SNMP V3 protocol configuration</td>
</tr>
<tr>
<td></td>
<td>Appendix A Troubleshoot Network Switch SNMP Issues</td>
<td>Updated the first paragraph and related figure for SNMP V1 and SNMP V3 protocol clarification</td>
</tr>
<tr>
<td>Revision</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Virtualization Server Alarms Configuration Parameters</td>
<td>New section containing parameters associated with Virtualization Server alarms</td>
</tr>
<tr>
<td></td>
<td>Virtual Machine Alarms Configuration Parameters</td>
<td>New section containing parameters associated with Virtual Machine alarms</td>
</tr>
<tr>
<td></td>
<td>Virtualization Data Acquisition Configuration Parameters</td>
<td>New section containing parameters associated with Virtualization Data Acquisition</td>
</tr>
<tr>
<td></td>
<td>OPC UA Communication</td>
<td>Renamed this chapter from OPC Application Certificate to OPC UA Communication and organized the chapter into subsections, Client/Server Connection Sequence and Application Certificate Sharing</td>
</tr>
<tr>
<td></td>
<td>Control Server Support</td>
<td>Updated this chapter to replace content specific to Thin Client HMI with more generic content for Control Server support</td>
</tr>
<tr>
<td></td>
<td>Control Server Configuration</td>
<td>New chapter containing ToolboxST configuration procedures</td>
</tr>
<tr>
<td></td>
<td>Virtualization Platform Health Information</td>
<td>New section to provide details on the Virtualization Platform node of the Control System Health Viewer, which displays the health information for Control Server</td>
</tr>
<tr>
<td></td>
<td>Appendix A Troubleshoot Network Switch SNMP Issues</td>
<td>Existing Troubleshooting section content moved to Appendices</td>
</tr>
<tr>
<td></td>
<td>Appendix B Connect to Server with vSphere Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix C Connect to vCenter Web Client</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix D Identifying Server Hardware Issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix E Resolve Failure to Get vSphere Data Issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix F Troubleshooting vCenter Alarm Monitoring Issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix G Trending Control System Health Data Example</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>Licensing</td>
<td>Updated content to state that CSH server can be licensed with a software key</td>
</tr>
<tr>
<td></td>
<td>Network Health Data Acquisition Configuration Parameters</td>
<td>Updated the definition of Switch SNMP Data Request Rate and Local HMI Management Address, and added a Note to further explain the Network Monitor rate settings and how to tune the parameters to avoid an HMI freezing up</td>
</tr>
</tbody>
</table>
## Related Documents

<table>
<thead>
<tr>
<th>Doc #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6700</td>
<td>ToolboxST User Guide for Mark Controls Platform</td>
</tr>
<tr>
<td>GEI-100693</td>
<td>WorkstationST Network Monitor</td>
</tr>
<tr>
<td>GEI-100828</td>
<td>WorkstationST OPC UA Server</td>
</tr>
</tbody>
</table>

## Acronyms and Abbreviations

- **CSH**: Control System Health
- **DTM**: Device Type Manager
- **HMI**: Human-machine Interface
- **NIC**: Network Interface Card
- **NTP**: Network Time Protocol
- **PDH**: Plant Data Highway
- **RAID**: Redundant Array of Independent Disks
- **SDI**: System Data Interface
- **SNMP**: Simple Network Management Protocol
- **TMR**: Triple Modular Redundant
- **UDH**: Unit Data Highway
- **UPD**: Universal Serial Bus Protection Device
- **USB**: Universal Serial Bus
- **VLAN**: Virtual Area Network
### Contents

1. Overview .................................................................................................................. 7
   1.1 Data Flow ........................................................................................................... 9
   1.2 Licensing ............................................................................................................ 11

2. CSH Server ................................................................................................................. 12
   2.1 Configuration ...................................................................................................... 12
   2.2 Alarm Configuration .......................................................................................... 14
   2.3 Virtualization Server Alarms Configuration Parameters .................................. 20
   2.4 Virtual Machine Alarms Configuration Parameters ......................................... 21
   2.5 Virtualization Data Acquisition Configuration Parameters ......................... 21
   2.6 Remote Desktop Protocol (RDP) Connections Threshold Alarm ................... 22

3. Network Configuration ............................................................................................... 23
   3.1 Triple Modular Redundant (TMR) Mark Vle Controller Example .................... 23
   3.2 Redundant HMI Example without HMI Trunk Ports ...................................... 26
   3.3 Redundant HMI Example with HMI Trunk Ports ............................................. 29
   3.4 Other Device Type Port Configurations ............................................................ 32
   3.5 Upgrade Network Switch Configuration from ControlST V04.06 or Earlier ....... 35

4. Switch Management Network Support .................................................................... 38
   4.1 Add Management Network to System Topology .............................................. 39
   4.2 Configure Network Switch Configurations to Use Management Network ... 41
   4.3 Network Switch Layout Overview and Configuration ...................................... 44
   4.4 Switch Stacking and Hardware Monitoring ...................................................... 54
   4.5 Configure Local HMI Management Address .................................................... 71
   4.6 Add Local HMI Management Address to PDH Adapter in Workstation ....... 72

5. Configure Local HMI Management Address for Systems without Switch Management Network ..... 73
   5.1 Configure Local HMI Management Address in CSH Feature ........................... 73
   5.2 Add Local HMI Management Address to PDH Adapter in Workstation ....... 74

6. Network Switch SNMP Configuration .................................................................. 75
   6.1 New System Configuration .............................................................................. 75
   6.2 ControlST Upgrade ......................................................................................... 85
   6.3 Network Switch Replacement (Upgrade) ......................................................... 86

7. Control Server Support .............................................................................................. 87
   7.1 Control Server Monitoring Overview ............................................................... 87
   7.2 Control Server Configuration Overview .......................................................... 90

8. Thin Client HMI Support ............................................................................................ 91
   8.1 Create HMI Server Group ............................................................................... 91
   8.2 Configure Workstations Running as Virtual Machines ................................. 93
   8.3 Configure Network Switch Ports Connected to Server ................................... 94
   8.4 Configure Network Switch Ports Connected to Thin Client Terminals .......... 95
   8.5 Server and Thin Client Terminal Alarms ............................................................ 96

9. Control Server Configuration .................................................................................... 97
   9.1 Add New Control Server .................................................................................. 97
   9.2 Add Components to Existing Control Server .................................................. 106
   9.3 Virtualization Server Set Configuration ......................................................... 110
   9.4 Virtualization Server Configuration ............................................................... 113
   9.5 Virtual Machine Configuration ....................................................................... 120
   9.6 Thin Client Configuration ............................................................................... 123

10. OPC® UA Communication ...................................................................................... 127
    10.1 Client/Server Connection Sequence ............................................................... 127
    10.2 Application Certificate Sharing ...................................................................... 128

11. Control System Health Viewer ............................................................................... 129
    11.1 Virtualization Platform Health Information ................................................. 131
    11.2 WorkstationST Computer Health Information ............................................. 141
    11.3 Controllers Health Information ..................................................................... 142

Instruction Guide

Public Information

GEI-100834P
1 Overview

Beginning with ControlST* V04.07, a Control System Health (CSH) management system is included that provides access to real-time data and online health status. This management system collects health data from the many different device types that make up the control system. It presents this data in a unified system view that allows the user to view the overall system status and drill down to locate issues with individual devices from a single tool.

The CSH management system can display the health of various components on the Unit Data Highway (UDH), Plant Data Highway (PDH), and IONet. The system health is a collection of the health of the HMI and historian computers, the Mark* VIe and VIeS controllers, EX2100e and LS2100e controllers, network switch, I/O packs, power supply, NTP (time synchronization) status, and integration into the alarm system. If health is not available directly, then it can be inferred from the available parameters.

System health data is collected and displayed in the following groups:

- Computer Health provides health data for the critical hardware components of the system computers, as well as remote desktop connection monitoring.
- Controllers provides health data for all of the controllers and I/O packs in the system.
- Networks provides device communication status and switch connection information for each computer and controller.
- Network Time Protocol (NTP) provides the overall status of the time synchronization for the system.
- WorkstationST* provides the status of the GE ControlST Software Suite services running on the system computers.

The CSH management system has two components: a CSH server and a CSH viewer client.

The CSH server (WorkstationST application):

- Supports auto configuration, based on the system
- Has access to servers, workstations, UDH and PDH switches, Mark VIe, Mark VIeS, EX2100e, and LS2100e control systems (including controllers, I/O packs, and power supplies)
- Has access to the health information
- Generates alarms based on health information
- Has the Alarm Server connect as a client to get the CSH alarms
- Functions independently from the viewer
- Gets Simple Network Management Protocol (SNMP) data from network switches (UDH and PDH), servers, and workstations

**Note** SNMP is used to manage devices on internet protocol networks.

- Gets IONet, controller, and I/O pack health information over secure system data interface (SDI)
- Gets controller, I/O pack diagnostic alarms
- Gets NTP status for every device (workstations, servers, and controllers)
- Is a standard component as a part of an enabled computer with the WorkstationST application
CSH viewer (stand-alone application):

- Is packaged separately
- Provides overall system health view (the Tree View can be expanded to display the I/O pack)
- Follows NAMUR guidelines to display health

Note  NAMUR is an international user association of automation technology in process industry.

- Provides system NTP view
- Provides network specific view (including IONet)
- Can connect to the server only with proper access control (log on, privileges, and such)
- Can connect to the server if the purchased licensed connection count has not been exceeded

Note  For viewers connecting from a different computer, the viewer's OPC UA certificate must be added to the CSH server's certificate store by an administrator.

The CSH management system includes the following:

- Network asset health:
  - Network switch health (port status and connected device status)
  - Network topology (devices connected to correct switch and port)
  - NTP status of all NTP capable devices
- Asset Time Synchronization health: NTP status of the time servers and all NTP capable devices in the system
- Computer asset health:
  - Workstation computer health (such as network communication status)
  - Server health
- Software asset health: key software programs health
- Control system hardware health:
  - Controller health (diagnostic alarms, IONet health, I/O module communication status and diagnostics)
  - I/O pack health
  - Power distribution health

The CSH management system is used by plant operators and maintenance personnel for quick and continuous monitoring of health in the entire system. The CSH management system supports multiple operating systems (OS). For a list of recommended and supported OS, refer to the ToolboxST User Guide for Mark Controls Platform (GEH-6700 or GEH-6703), the section Computer Recommendations.

Note  This system allows access to more information for easy troubleshooting.
1.1 Data Flow

The CSH management system processes and distributes live data through the following CSH features:

- **Network Monitor** provides network and device data. When CSH is enabled, the WorkstationST Network Monitor cannot be enabled. Thus, CSH provides network monitoring for legacy Mark VI control and external EGD devices, such as PLCs. Refer to the *WorkstationST Network Monitor Instruction Guide* (GEI-100693) for more information.
- **Controller Health Monitor** provides health data for each controller and I/O pack in a Mark VIe, EX2100e Excitation, or LS2100e Static Starter control system.
- **NTP Monitor** provides network time synchronization status.
- **Computer Health Monitor** provides health data of networks, processors, hard disks, and remote desktop connections, as well as WorkstationST process health.
- **Control Server Monitor** provides control server health data.

The following diagram illustrates how live data values and CSH diagnostics flow among the various features in the WorkstationST application.
The live values provided to the CSH Viewer are made available from the WorkstationST OPC UA server. The viewer reads the OPC UA server namespace to display the tree nodes under the Controllers, Networks, NTP, Computer Health, and WorkstationST tree nodes. Where redundant controllers are present, the viewer shows information for each redundant component as follows:

**Health Data**

The CSH Viewer uses OPC UA to communicate to the OPC UA Server running on the same computer as the CSH feature. When displaying the viewer, the colored icon in the tree view represents the status of the item.

- Unhealthy
- Error
- Warning
- OK

*Note* Refer to the section *Control System Health Viewer.*
When the path to the collected data is not healthy, the variable values display in red in the viewer.

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the operational status of the Controller</td>
<td>0</td>
</tr>
<tr>
<td>Indicates whether the Controller state is being actively updated</td>
<td>0</td>
</tr>
<tr>
<td>The designated Controller from this controller's point of view</td>
<td>0</td>
</tr>
<tr>
<td>The number of Forces active in the Controller</td>
<td>0</td>
</tr>
<tr>
<td>Indicates whether the Controller is reporting a Hardware failure</td>
<td>False</td>
</tr>
<tr>
<td>The reason for the Controller Hardware Alarm</td>
<td>0</td>
</tr>
<tr>
<td>Controller percent idle time</td>
<td>0</td>
</tr>
<tr>
<td>The Controller Is in the Controlling State</td>
<td>False</td>
</tr>
<tr>
<td>The Controller Frame Synchronization Status</td>
<td>True</td>
</tr>
<tr>
<td>Controller Online Status</td>
<td>True</td>
</tr>
<tr>
<td>The Controller's UDH Network EGD Health</td>
<td>True</td>
</tr>
<tr>
<td>Indicates the presence of diagnostics in the Controller's diagnostic alarm queue</td>
<td>False</td>
</tr>
<tr>
<td>Health Status of the Controller</td>
<td>Error</td>
</tr>
</tbody>
</table>

When the data is healthy, it displays in green, as shown in the following figure.

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices is Online</td>
<td>True</td>
</tr>
<tr>
<td>NTP Responding to requests</td>
<td>True</td>
</tr>
<tr>
<td>NTP Synchronization Status</td>
<td>True</td>
</tr>
<tr>
<td>NTP offset from time reference</td>
<td>0</td>
</tr>
<tr>
<td>The NTP status for the Device</td>
<td>OK</td>
</tr>
<tr>
<td>NTP Stratum Level</td>
<td>0</td>
</tr>
<tr>
<td>NTP Time Source</td>
<td>172.20.99.135</td>
</tr>
</tbody>
</table>

The OPC UA protocol provides for a status code for each live value. This status code drives the live values.

### 1.2 Licensing

The CSH server requires a ControlST license with a CSH license count greater than zero (0). The license can be purchased for 1 to 255 viewers. The server allows up to that number of connections if CSH variables are mapped on EGD for use on CIMPLICITY HMI screens.

**Note** For more information on license keys and the license ordering process, refer to the *ControlST Software Suite License Key Ordering Flow Diagram* (GHT-200060) and *How to Order ControlST Software and License Keys* (GHT-200048).
2 CSH Server

2.1 Configuration

➢ To enable the CSH server

From the **ToolboxST System Editor Tree View**, select the system item.

From the **Property Editor**, expand the **Control System Health** section and select the **Primary WorkstationST** from the drop-down menu.

This setting allows the CSH viewer to know where to connect to reach the CSH server. When the CSH viewer is running on a computer that is part of a system configured in the ToolboxST* application, the viewer can determine where the CSH server resides by asking the local WorkstationST application.

*Note* The CSH viewer also provides a menu item to allow the user to enter the CSH server’s host name or address.
From the Workstation ST General tab Tree View, select Features.

From the Summary View, select Control System Health and set to True.

The Control System Health tab displays.

The CSH management system requires minimal configuration. The feature collects a predefined set of data for all of the devices in the system and makes this data available to the user through the Control System Health Viewer and to other clients through OPC UA. The CSH management system also generates alarms when the data values exceed predefined threshold values.

**Note** Refer to the section *Alarm Configuration* for more information.
2.2 Alarm Configuration

The CSH management system monitors conditions and generates alarms when error and warning conditions are detected. These alarms must be collected and displayed by the alarm system in order for a user to act on them. The CSH server acts as a server of the CSH alarms.

Note The WorkstationST Alarm Server must be configured to establish a connection to the CSH server in order to receive alarm messages.

➢➢ To configure the Alarm Server to collect CSH alarms: from the ToolboxST System Editor Tree View, double-click the WorkstationST computer running the Alarm Server (wkstn1).

This configures the Alarm Server to connect to the CSH server and get its alarms. One workstation in the system can be configured to host the CSH server and that workstation’s hostname or IP address is entered here. Each Alarm Server in a redundant Alarm Server system configuration should be configured to connect to the CSH server, which allows all Alarm Servers to collect and maintain a consistent set of CSH alarms.

Note The connection parameter also allows the connection to the Network Monitor feature to be specified instead of CSH. One workstation in the system can be configured to host either CSH or the Network Monitor. CSH is replacing the Network Monitor and provides all of the functionality of the Network Monitor plus the additional CSH status information and alarms. The Network Monitor is being maintained for existing sites that do not wish to upgrade.

The CSH management system generates alarms when the data values exceed predefined threshold values. These threshold values can be modified in order to determine the point at which to generate alarms for each condition. Many parameters also have a delay value associated with them. The delay value is used to reduce the sensitivity to momentary conditions and avoid dithering alarms in situations where the value is regularly crossing the threshold value and returning to the normal range in a short period of time. A lower delay reduces the amount of time it takes to report an error condition but also increases the sensitivity to momentary spikes in the parameter value. A higher delay value increases the time it takes to report the alarm condition and decreases the sensitivity to momentary value spikes.

As an example, consider the case where the Computer CPU Usage parameters are set to the default values with the Warning threshold at 85%, the error threshold at 95%, and a delay of three (3) scans as shown in the following figure.
The CSH management system will generate a warning if the CPU usage stays above 85% for three consecutive data scans, which is approximately 90 seconds. If the CPU usage spikes above 85% for one scan and then returns to normal, no alarm is generated and the scan counter is reset. If the CPU usage spikes above 85% for more than three scans (90 seconds) a warning alarm will be generated and a warning condition will be indicated in the Control System Health Status Viewer. The alarm will return to the normal state and the warning will be cleared as soon as the value drops below 85%. The warning will not occur again until the value exceeds 85% for another three consecutive data scans. Note that the delay period applies to both Warning and Error conditions simultaneously; Warnings and Alarms can occur after the value has exceeded the Warning threshold for the configured delay period. As an example, if CPU usage exceeds the warning threshold for 90 seconds a Warning alarm is generated. If the CPU usage then increases beyond the Error threshold, on the next scan an Error alarm is generated and the Warning alarm remains active. If the CPU usage falls below the Error threshold level but remains above the Warning threshold, the Error alarm will return to normal and the Warning alarm will remain active until the value drops below the Warning threshold. Alarms will not be generated again until the value exceeds the Warning threshold for the configured delay period.

As another example, assume the delay value is set to zero. This allows the Warning and Error alarms to be generated as soon as the value crosses the threshold values. This may be desirable for some parameters, but in the case of CPU usage this would cause a lot of nuisance alarms since it would normally be expected that the CPU usage will spike to levels around 100% during normal operation. In the case of CPU usage, momentary spikes in values are expected, but prolonged periods of high CPU usage may indicate a problem.
To display the CSH parameters

Select the Control System Health tab.

The Summary View displays the Control System Health parameters and alarms.

Control System Health parameters and alarms are provided in the following list.
2.2.1 Computer Health Alarm Configuration Parameters

The parameters associated with the Computer Health alarms are as follows:

**Computer Health Alarms**

**Battery Status Errors** is the list of battery states that will generate an error alarm when the battery transitions to one of these states. The default is Degraded, InstallError, PowerSaveLowPower.

**Battery Status Warnings** is the list of battery states that will generate a warning alarm when the battery transitions to one of these states. The default is Warning, OffLine, OffDuty.

**Fan Status Errors** is the list of fan states that will generate an error alarm when the fan transitions to one of these states. The default is Degraded, InstallError, PowerSaveLowPower.

**Fan Status Warnings** is the list of fan states that will generate a warning alarm when the fan transitions to one of these states. The default is Warning, OffLine, OffDuty.

**Free Physical Memory Percentage Alarm Delay** is the number of scans that must be performed while the free physical memory percentage is in the warning or error state, before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Free Physical Memory Percentage Error Threshold** is when the percentage of available memory reaches or falls below this value, an error alarm is generated. The default value is 5.

**Free Physical Memory Percentage Warning Threshold** is when the percentage of available memory reaches or falls below this value, a warning alarm is generated. The default value is 10.

**Computer Health Disk Alarms**

**Current Queue Length Alarm Delay** is the number of scans that must be performed while the disk current queue length is in the warning or error state, before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Current Queue Length Error Threshold** is when the number of I/O operations waiting for the hard drive to become available, in relation to the number of spindles, reaches or exceeds this value indicating the disk may be bottlenecked and an error alarm is generated. The default value is 3.

**Current Queue Length Warning Threshold** is when the number of I/O operations waiting for the hard drive to become available, in relation to the number of spindles, reaches or exceeds this value indicating the disk may be bottlenecked and a warning alarm is generated. The default value is 2.

**Free Space Percentage Alarm Delay** is the number of scans that must be performed while the percentage of free disk space is in the warning or error state, before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Free Space Percentage Error Threshold** is when the percentage of free space of the selected logic disk reaches or falls below this value, the disk is running very low on space and an error alarm is generated. The default value is 5.

**Free Space Percentage Warning Threshold** is when the percentage of free space of the selected logic disk reaches or falls below this value, the disk is running low on space and a warning alarm is generated. The default value is 15.

**Idle Time Percentage Alarm Delay** is the number of scans that must be performed while the disk idle time percentage is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Idle Time Percentage Error Threshold** is when the percentage of time the disk was idle during the sample interval reaches or falls below this value, indicating the disk system is saturated and an error alarm is generated. The default value is 10.

**Idle Time Percentage Warning Threshold** is when the percentage of time the disk was idle during the sample interval reaches or falls below this value, indicating the disk system is saturated and a warning alarm is generated. Default value is 20.
Computer Heath Network Adapter Alarms

**I/O Mb/Sec Alarm Delay** is the number of scans that must be performed while the I/O Mb/Sec rate is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**I/O Mb/Sec Error Threshold** is when the rate at which bytes are sent and received over each network adapter, including framing characters, reaches or exceeds this value, indicating that the network is saturated and an error alarm is generated. The default value is 80.

**I/O Mb/Sec Warning Threshold** is when the rate at which bytes are sent and received over each network adapter, including framing characters, reaches or exceeds this value, indicating that the network is becoming saturated and a warning alarm is generated. The default value is 70.

**Output Queue Length Alarm Delay** is the number of scans that must be performed while the length of the output packet queue is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Output Queue Length Error Threshold** is when the length of the output packet queue, in packets, reaches or exceeds this value, indicating that the network is saturated and an error alarm is generated. The default value is 3.

**Output Queue Length Warning Threshold** is when the length of the output packet queue, in packets, reaches or exceeds this value, indicating that the network is becoming saturated and a warning alarm is generated. The default value is 2.

**Utilization Alarm Delay** is the number of scans that must be performed while the ratio of current network traffic to the maximum traffic that the port can handle is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Utilization Error Threshold** is when the ratio of current network traffic to the maximum traffic that the port can handle reaches or exceeds this value, indicating that the network is busy and a warning alarm is generated. The default value is 99.

**Utilization Warning Threshold** is when the ratio of current network traffic to the maximum traffic that the port can handle reaches or exceeds this value, indicating that the network is becoming busy and a warning alarm is generated. The default value is 95.

Computer Heath Processor Alarms

**Execution Time Percentage Alarm Delay** is the number of scans that must be performed while the time percentage is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Execution Time Percentage Error Threshold** is when the percentage of elapsed time the processor spends executing a non-idle thread reaches or exceeds this value, indicating the processor is overwhelmed and an error alarm is generated. The default value is 95.

**Execution Time Percentage Warning Threshold** is when the percentage of elapsed time the processor spends executing a non-idle thread reaches or exceeds this value, indicating the processor is becoming overwhelmed and a warning alarm is generated. The default value is 85.

**Interrupt Time Percentage Alarm Delay** is the number of scans that must be performed while the interrupt time percentage is in the warning or error state before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Interrupt Time Percentage Error Threshold** is when the time the processor spends receiving and servicing hardware interruptions during specific sample intervals reaches or exceeds this value, indicating a possible hardware issue and generating an error alarm. The default value is 15.

**Interrupt Time Percentage Warning Threshold** is when the time the processor spends receiving and servicing hardware interruptions during specific sample intervals reaches or exceeds this value, indicating a possible hardware issue and generating a warning alarm. The default value is 15.
2.2.2 Controller Health Alarm Configuration Parameters

The parameters associated with the Controller Health alarms are as follows:

**Controller Health Alarms**

**Idle Time Alarm Delay** is the number of scans that must be performed while the controller idle time is in the warning or error state, before an alarm is generated. The default value is 3. One scan is approximately 30 seconds.

**Idle Time Error Threshold** is when the controller idle time reaches or falls below this value, an error alarm is generated. The default value is 10.

**Idle Time Warning Threshold** is when the controller idle time reaches or falls below this value, a warning alarm is generated. The default value is 15.

**General**

**Auto Reset of Alarms** when enabled automatically resets acknowledged CSH alarms in the Normal state.

2.2.3 Network Health Alarm Configuration Parameters

The parameters associated with the Network Health alarms are as follows:

**Network Monitor Alarms**

**Enable Alarm On Intrusion Detection Threshold Exceeded** when enabled generates an alarm when the intrusion detection counter delta threshold is exceeded.

**Enable Alarm On Loss of Device Communication** when enabled generates an alarm whenever network communications are lost with a device.

**Enable Alarm On Topology Error** when enabled generated an alarm when a device is not connected to its configured port.

**Enable Alarm On Unknown Device Connected** when enabled generates an alarm when an unknown device is connected to any of the defined networks.

**Enable Event On Intrusion Detection Threshold Exceeded** when enabled generates an event when the intrusion detection counter delta threshold is exceeded.

**Enable Event On Loss of Device Communication** when enabled generates an event whenever network communications are lost with a device.

**Enable Event On Topology Error** when enabled generated an event when a device is not connected to its configured port.

**Enable Event On Unknown Device Connected** when enabled generates an event when an unknown device is connected to any of the defined networks.
2.2.4 Network Health Data Acquisition Configuration Parameters

The parameters associated with the Network Health data acquisition are as follows:

**Network Monitor Data Acquisition**

*Device Network Communication Status Request Rate (seconds)* is the number of seconds between device network communication status requests. Decreasing the rate makes detection of device communication status changes faster at the cost of using additional network bandwidth. Increasing the rate reduces the amount of network bandwidth used at the cost of slowing down the speed of detection of device communication status changes.

*Intrusion Detection Delta Threshold* is the delta of intrusion detection counter values over the device SNMP request period that will trigger an intrusion alarm or event.

*Switch SNMP Data Request Rate* is the number of seconds between SNMP queries of the network switches. Decreasing the rate makes detection of switch port status changes and connected device changes faster at the cost of using additional network bandwidth and increased CPU usage on the host computer. Increasing the rate reduces the amount of network bandwidth used at the cost of slowing down the speed of detection of switch port status and connected device status.

*Local HMI Management Address* is the address configured in the switch access list (ACL) for SNMP requests.

---

**Note** The Network Monitor Data Acquisition request rate settings are used to tune the performance of the Network Health monitoring based on the size of the system and the capabilities of the hardware hosting the Control System Health feature. Lower Request Rates (polling periods) increase the frequency of the data requests and provides faster detection of issues at the expense of consuming higher network bandwidth and CPU resources on the host computer. Higher values for the Request Rates results in a lower frequency of requests, which ultimately results in slower updates while consuming less network and host computer resources. The default rates provide very fast updates in small systems, but can easily overwhelm the host computer in a large system. The Request Rate settings are used to tune the Network Health monitoring to achieve the best compromise of performance and resource usage based on the priorities of the site. If a site wants to minimize detection delays and is willing to accept higher network bandwidth usage and CPU usage on the host computer, they can increase the polling frequency by decreasing the Request Rate setting. If the site is sensitive to network bandwidth usage and needs good performance for other applications on the host computer, they can reduce the polling frequency by increasing the Request Rate setting.

Many factors come in to play and each site is different so there is no simple calculation for performance versus resource usage. The best way to determine actual system behavior is to adjust the rate settings until an acceptable balance of performance and hosting computer resource usage is achieved at the site.

---

2.3 Virtualization Server Alarms Configuration Parameters

The parameters associated with the Virtualization Server Alarms are as follows:

**Virtualization Server Alarms**

*Enable critical Virtual Machine not running alarms* specifies if alarms will be generated when critical VMs are either stopped or running in an abnormal state.

*Enable unknown Virtual Machine alarms* specifies if alarms will be generated for VMs that are found on the Server Set that are not configured in the Virtualization Server Set in ToolboxST.

*Enable Virtual Machine migration events* specifies if events will be generated when a VM is migrated from one server to another.

*Generate vCenter unacknowledged Alerts alarm* specifies if an alarm will be generated when one or more unacknowledged vSphere alarms with an Alert status are detected in the vCenter alarm queue.

*Generate vCenter unacknowledged W arnings alarm* specifies if an alarm will be generated when one or more unacknowledged vSphere alarms with a Warning status are detected in the vCenter alarm queue.
**Server Datastore low free space alarm threshold** specifies the low datastore free space threshold. Alarms are generated if the percentage of free space of any server datastore drops below the configured threshold level.

**Server High CPU Usage alarm duration threshold in minutes** specifies the amount of time that the CPU usage must exceed the threshold value before an alarm will be generated.

**Server High CPU Usage alarm threshold in percent** specifies the threshold for the high CPU usage alarm. An alarm will be generated if the CPU usage exceeds the threshold for the configured duration.

**Server High Memory Usage alarm duration threshold in minutes** specifies the amount of time that the memory usage must exceed the threshold before an alarm is generated.

**Server High Memory Usage alarm threshold in percent** specifies the threshold for the high memory usage alarm. An alarm will be generated if the memory usage exceeds the threshold value for the configured duration.

**Server VSAN Datastore low free space alarm threshold** specifies the percentage of Virtual SAN datastore free space below which an alarm will be generated.

### 2.4 Virtual Machine Alarms Configuration Parameters

The parameters associated with the Virtual Machine Alarms are as follows:

**Virtual Machine Alarms**

**Virtual Machine High CPU Usage alarm duration threshold in minutes** specifies the amount of time that the CPU usage must exceed the threshold value before an alarm will be generated.

**Virtual Machine High CPU Usage alarm threshold in percent** specifies the threshold for the high CPU usage alarm. An alarm will be generated if the CPU usage exceeds the threshold for the configured duration.

**Virtual Machine High Memory Usage alarm duration threshold in minutes** specifies the amount of time that the memory usage must exceed the threshold before an alarm is generated.

**Virtual Machine High Memory Usage alarm threshold in percent** specifies the threshold for the high memory usage alarm. An alarm will be generated if the memory usage exceeds the threshold value for the configured duration.

**Virtual Machine low free disk space alarm threshold in percent** specifies the threshold at which the free disk space alarm is generated. An alarm will be generated if the free disk space for any virtual disk hosted by the Virtual machine drops below the configured threshold value.

**Virtual Machine uncommitted storage threshold in percent** specifies the threshold at which the uncommitted storage alarm is generated. An alarm will be generated if the Virtual Machine uncommitted storage drops below the configured threshold value.

### 2.5 Virtualization Data Acquisition Configuration Parameters

The parameter associated with Virtualization Data Acquisition is as follows:

**Virtualization Data Acquisition**

**Hypervisor Data Request Rate in seconds** specifies the number of seconds between data requests to the Virtualization Servers. Lowering the request period results in faster data updates at the expense of higher network bandwidth and resource usage, while increasing the request period results in slower data updates with reduced network bandwidth and resource usage.
2.6 Remote Desktop Protocol (RDP) Connections Threshold Alarm

CSH can monitor active Windows® connections to determine if sessions are remote using the Windows Remote Desktop Protocol (RDP). If the number of remote sessions falls below the threshold of 1 (if the remote connection count is 0), it generates an alarm.

**Note** Windows sessions that are local or through TCP connection (other than RDP) will not be determined as remote connections.

The *Monitor Active RDP Connections* property must be enabled to generate the alarm when the number of remote desktop sessions falls below the threshold.

**Attention** The feature is intended for use with Virtual Machine (VM) applications.

➢ To enable the RDP Connections Threshold Alarm: from the ToolboxST WorkstationST Component Editor General tab, set the Monitor Active RDP Connections property to **True**.
3 Network Configuration

The CSH management system uses the device to network switch port connection information associated with each network switch to detect network topology errors. The connection information is configured in the network switch device in the ToolboxST application. The CSH management system periodically queries the network switches to determine what devices are connected to its ports and generates a topology error if it detects that a device is connected to a port other than the one it is configured for. Most devices have a connection to a single network switch port, while workstations typically have redundant network connections and each connection may host multiple networks.

**Note** The device connections to each network switch are defined in the system 4108 drawing.

3.1 Triple Modular Redundant (TMR) Mark VIe Controller Example

Each controller in a TMR Mark VIe controller has a connection to a UDH port of a network switch. Typically the controllers are connected across multiple network switches to avoid losing all unit communications in the event of a single network switch failure.

➢ To create a connection between a controller and network switch port

1. From the ToolboxST **System Editor Tree View**, double-click the network switch (SW1) to open the **Component Editor**.
2. Select the desired Port’s Network Node for the appropriate controller.
From the **Tree View**, select the **General item**.

From the **Summary View**, select the **Network Component** cell for the desired **Port** (Port 18), click the ellipse, select the **Network Node** for the desired controller (**G2-R**), and click **OK**.
The Network Node displays.

Repeat the previous step using a different network switch (SW2 Port 20 and 21) and the other two controllers (G1–S and G1–T).
3.2 **Redundant HMI Example without HMI Trunk Ports**

Redundant HMI network connections are achieved by teaming two sets of Network Interface Cards (NIC) in the HMI computer. One set handles the PDH network and the other set handles the UDH network. Each NIC in the set is connected to a different switch to provide communications in the event of a switch failure. The following figure displays the physical connections in this arrangement.

This arrangement is configured in the network switch device by adding one connection to each port as specified.

➢ **To create a redundant HMI without HMI trunk ports**

1. From the ToolboxST System Editor Tree View, double-click the network switch (SW1) to open the Component Editor.

2. Select the desired Port’s Network Node for each workstation (Primary and Backup connections).
From the **Tree View**, select the **General** item.

From the **Summary View**, select the **Network Component** cell for the desired **Port** (Port 5), click the ellipsis, select the desired **Network Node** (wkstn1), and click **OK**.

---

**Note**  
Notice that workstations include both a Primary and Backup selection for each network connection.
Repeat the previous step until both Primary and Backup connections are made for both workstations.

Note that Ports 5 and 6 are designated as Primary ports and Ports 8 and 9 are designated as Backup ports. There is only one network connection per port.
3.3 Redundant HMI Example with HMI Trunk Ports

A simplified network uses VLAN tagging in the workstation NICs and the network switches to combine the PDH and UDH VLANs onto a common network connection, referred to as a trunk because multiple VLANs coexist on the same connection. Only one set of NICs is required to provide full PDH and UDH redundancy. The following figure displays the physical connections in this arrangement.

![Diagram showing PDH/UDH Primary and Backup ports with a network switch and a workstation]

**Note** Each port has both a PDH and UDH Network connection, and one port is designated as the Primary port while the other port is designated as the Backup port.

➢ To create a redundant HMI with HMI trunk ports: from the ToolboxST System Editor Tree View, double-click the network switch (SW1) to open the Component Editor.
From the **Tree View**, select the **General** item.

From the **Summary View**, select the **Network Component** cell for the desired **Port** (Port 5), click the ellipsis, select the desired **Network Node** (wkstn1), and click **OK**.
From the **Summary View**, select **Network_2** for the same **Port** (Port 5), click the ellipsis, select the **Network Node** (wkstn1) and click **OK**.

Note that the selection enforces the fact that **Network_2** must be different from **Network_1** and that the **Network_2** redundant connection type (Primary or Backup) must match the **Network_1** type, which is also enforced by the selection dialog. In this example the **Network_1** connection was defined as **UDH Primary** so the selection dialog only allows the choice of **PDH Primary** for **Network_2**.

Repeat these steps on another **Port** (such as **Port 7**) for the redundant network.

The results of the configuration display.
3.4 Other Device Type Port Configurations

Most devices connected to the switch ports are defined in the system configuration and are presented in the network component drop-down list for each port (also referred to as Native devices). The CSH management system must also be aware of customer devices connected to the network switches that are not defined in the ToolboxST system configuration, in addition to switch-to-switch communication ports and devices that may not always be online, such as network printers. The port connection parameter is used to support the special case port connection types described in the following sections.

3.4.1 Default Connection

The Default_NativeDeviceConnectionOrNotUsed setting is the default port connection designation. This setting is used if the connected device is defined in the ToolboxST system (referred to as a Native device) or if no connection is made to the port.

3.4.2 Trunk Port

A Trunk port is a port that carries network traffic for all of the VLANs for which the switch is configured (PDH, UDH, MDH, and so forth). Trunk ports are used to connect the switches and allows them to send network traffic between them. Trunk ports are critical to the network operation; the CSH management system will generate an alarm if a designated trunk port is down. All port entries allow a free form description to be added. This description is displayed in the Network Status Viewer to help identify the switch-to-switch connections. This description is also included in the alarm description of any alarms that are generated for this port, as shown in the following figure.
3.4.3 **Peripheral Device Connection**

Some devices are not expected to be online and communicating at all times and are therefore not critical to the process. An example would be a network printer. The port that the network printer is connected to will be up when the printer is on and down when the printer is off. The PeripheralDeviceConnection designation is used to specify device connections to non-critical devices.

*Note* Alarms are not generated when ports specified as peripheral device connection ports are down.

3.4.4 **Third-party Critical Device Connection**

Customer equipment that is connected to the system network switches but not defined in the ToolboxST system is given the ThirdPartyCriticalDeviceConnection designation. Similar to the Trunk Port, the port description is displayed in the Network Status Viewer to help identify the switch-to-switch connections, and this description is also included in the alarm description of any alarms that are generated for this port.

*Note* Alarms are generated whenever a port designated as a third-party critical device connection is down.

3.4.5 **Server**

The Server port connection type is used to designate switch ports that are connected to devices that host a hypervisor and one or more Virtual Machines (VM). In this situation, the correlation to IP and MAC address is lost and multiple MAC addresses may display on the port and multiple IP addresses may respond to the same MAC address. Configuring a port as a Server signals the Network Monitor to ignore the MAC addresses on the port; only the port status is monitored and an alarm is generated if the port is down.

*Note* The Server port connection type is only used for third-party devices with a hypervisor. Native servers, like Control Servers and Security Servers, are represented by devices in the system configuration, while third-party devices have no corresponding device type in ToolboxST. As a result, these devices can only be detected and monitored at the port level.
3.4.6 Thin Client

This connection type is for legacy system support only. Thin Clients should be configured using the Thin Client device in ToolboxST.

Attention

A Control Server consists of the servers and VMs hosted by them. User access to the VMs is facilitated using Thin Client terminals on the plant network. When the Control Server was first introduced, there was no corresponding Thin Client device in ToolboxST and the Thin Client port connection type was used to specify ports with Thin Client terminal connections. Do not use this connection type. Instead, add Thin Client devices to the system configuration in ToolboxST so that the Thin Client port connection and IP address can be defined and the Thin Client status can be fully monitored. Only the status of the port is monitored when the Thin Client connection type is used and an alarm is generated if the port is down.

3.4.7 Gateway

The Gateway port connection type is used for switch ports connected to critical third-party networks. By definition, the devices on the third-party network are unknown so the MAC addresses associated with these ports are ignored. The Gateway port connection type monitors the status of the port and generates an alarm when the port is down. This connection type is used when the connected network is critical to the plant operation. This connection type can also be used for connections to network routers or hubs.

3.4.8 Temporary Gateway

The Temporary Gateway port connection type is used for switch ports connected to non-critical third-party networks. By definition, the devices on the third-party network are unknown so the MAC addresses associated with these ports are ignored. The Temporary Gateway port connection enables monitoring of the port status but an alarm is not generated if the port is down.
3.5 Upgrade Network Switch Configuration from ControlST V04.06 or Earlier

With the release of ControlST V04.07, the Network Switch component of the ToolboxST application was enhanced to move configuration of each port connection from each device’s network adapter to the network switch Component Editor. The following examples show network configurations for a V04.06 system for a G1 and an S1 controller, as well as an EWS1 WorkstationST computer. Each has connections to a network switch component SW1.

After upgrading the system to V04.07, when the network switch device is opened it pre-populates the switch port connection information with the information from the devices. The device port connection information is no longer shown at each device network adapter. However, the information is still available in the EGD configuration server published files so that V04.06 and earlier versions of the WorkstationST application, that may not have been upgraded, can continue to have working Network Monitor features.

**Note** Only V04.07 and later Network Monitor or Control System Health will use this configuration change.

This device configuration for legacy network monitors cannot be changed with V04.07. If a change is made to the new switch centric port configuration, these older network monitors will not adapt to these changes.

The following figure provides an example of G1 settings in a ToolboxST version earlier than V04.07.
The following figure provides an example of S1 settings in a ToolboxST version earlier than V04.07.

![S1 Settings Example](image1)

- **Adapter Settings**
  - Enabled: True
  - Host Name: S1
  - IP Address: 192.168.101.11
  - Wire Speed: Auto

- **Network Settings**
  - Network: UDH
  - Subnet Mask: 255.255.255.0

- **Network Switch Connection Settings**
  - Network Switch: SW1
  - Port Number: 2

- **Network Switch Connection Settings (S)**
  - Network Switch: SW1
  - Port Number: 13

- **Network Switch Connection Settings (T)**
  - Network Switch: SW1
  - Port Number: 14

The following figure provides an example of EWS1 UDH settings in a ToolboxST version earlier than V04.07.

![EWS1 UDH Settings Example](image2)

- **Network Settings**
  - Network: UDH
  - Subnet Mask: 255.255.255.0

- **Network Switch Connection Settings**
  - Network Switch: SW1
  - Port Number: 3

- **Network Switch Connection Settings - Backup**
  - Backup Network Sw: SW1
  - Backup Port Number: 16
The following figure provides an example of EWS1 PDH settings in a ToolboxST version earlier than V04.07.

![Diagram of EWS1 PDH settings]

The following figure provides an example of SW1 after the upgrade to V04.07.

![Diagram of SW1 after upgrade]

*Instruction Guide GEI-100834P 37*
Switch management and periodic data collection from the switches through SNMP has traditionally been done over the PDH (plant scope) network. The switches have traditionally been given PDH IP addresses and the management interface has been associated with the PDH VLAN in the switches. This approach exposes the network switch management interface to any device on the PDH network.

A more secure architecture uses an isolated Switch Management network for switch configuration management and data gathering. Further security can be achieved by limiting access to this network to a single PC in the system. Sites configured to use a separate Switch Management network implement this arrangement with enhanced switch and router configurations. The ToolboxST application and the WorkstationST features have been modified to support this new network topology.

A series of steps must be performed to configure the WorkstationST CSH feature to support systems with an isolated Switch Management network. As an example, we start with this simple system containing a PDH (plant scope) and UDH (unit scope) network, two network switches, a single Workstation PC and two controllers.
4.1 Add Management Network to System Topology

➢ To add a new network to the system

From the Tree View, right-click the system icon, select Insert New and Network.

From the New Network dialog box, enter a Name (the convention is to use MGH) and Description (such as Switch Management).

Click OK.

From the Property Editor, select Scope and select Management from the drop-down list.

Select Media and select Ethernet from the drop-down menu.

Select Transport and select IP from the drop-down list.
System Topology with new Network
4.2 Configure Network Switch Configurations to Use Management Network

Specify the management network and the management address for all of the switches in the system.

➢ To configure a network switch

1. From the System Editor Tree view, double-click a Network Switch to display the Component Editor.

2. From the Component Editor Tree view, select General (top-level node) to display the Property Editor containing the network switch configuration properties.

3. Select Management IP Address and enter the appropriate IP address.

4. Select Management Network and select MGH from the drop-down list.

5. Repeat this procedure for each network switch in the system.
The following table describes the properties that can be configured for network switches.

### Network Switch Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Holds the user entered description for the switch. This text is displayed in the switch ToolTips in the Network Status Viewer and should include the physical location of the switch in order to help maintenance personnel locate and identify the switch in the event of a failure.</td>
</tr>
<tr>
<td>GE Part Number</td>
<td>Optional setting</td>
</tr>
<tr>
<td>Host Name</td>
<td>Part of the communication path</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>Configured management IP address of the switch</td>
</tr>
<tr>
<td>Management Network</td>
<td>Network associated with the management interface of the switch</td>
</tr>
<tr>
<td>Number of Ports</td>
<td>Specifies the number of switch ports. Note that for a stacked switch arrangement, the total number of ports for both switches should be specified.</td>
</tr>
<tr>
<td>Protection</td>
<td>Shows access rights for the device</td>
</tr>
<tr>
<td>Switch Layout Type</td>
<td>Specifies the type of switch. If a switch type cannot be found that matches the actual switch, one of the generic switch types can be used. Unknown switch types may require trial and error in order to find a switch type that matches the behavior of the actual switch. Switch layout types are defined in the System Information Editor. For instructions to configure network switch layouts, refer to the section <a href="#">Network Switch Layout Overview and Configuration</a>.</td>
</tr>
<tr>
<td>Vendor Configuration Tool</td>
<td>Optional setting</td>
</tr>
<tr>
<td><strong>SNMP Overrides</strong></td>
<td>For instructions to configure the SNMP, refer to the section <a href="#">Network Switch SNMP Configuration</a>.</td>
</tr>
<tr>
<td>SNMP Local Parameter Override</td>
<td>When True, these local switch SNMP settings are used. When False, the SNMP settings from the Network Monitor are used.</td>
</tr>
<tr>
<td>SNMP Mode</td>
<td>Sets SNMP mode used to read SNMP data from the network switches</td>
</tr>
<tr>
<td>SNMP V1 Community</td>
<td>SNMP V1 Community name configured in the network switches. This value must match the SNMP Community value configured in the switch.</td>
</tr>
<tr>
<td>Switch SNMP Data Request Rate</td>
<td>Number of seconds between SNMP queries of the network switches</td>
</tr>
</tbody>
</table>

The Summary View displays all of the switches connected to the management network, as displayed in the following figure.
4.3 Network Switch Layout Overview and Configuration

Beginning with ControlST V07.06.00C, Network Switch Layouts provide enhanced network switch management features. Network Switch Layouts provide the mapping between the internal switch interfaces and the physical switch ports, which enables the CSH feature to read the switch data over SNMP and display the data with the correct physical port location.

**Note** This feature was also added to some previous versions of ControlST and single-product releases. Refer to the table *Network Switch Layout Version Compatibility* for a complete version compatibility list.

Two types of Network Switch layouts are supported:

- **GE standard switch layout definitions**: standard switch layout definitions that are provided as part of the ControlST product. The standard switch layout files correspond to the standard switch types qualified for NetworkST. GE standard layouts cannot be modified.

- **Custom switch layout definitions**: custom switch layouts can be created to support non-standard switch types.

The use of switch layouts has been designed to provide the following improvements:

- **Support for newly qualified switch types independent of ControlST releases**: in previous ControlST versions, the network switch layouts were hard coded in the release. Support for newly qualified switches was only available as part of the next ControlST release and required, at a minimum, an update of ToolboxST and WorkstationST. ControlST V07.06.00C and later (or previous versions specified in the table *Network Switch Layout Version Compatibility*) moved the switch-specific code to a switch layout file. The switch layout file is updated as new switches are qualified, and this file can be sent to existing sites that need to support the new switch type independently of the ControlST release cycle and without the need to upgrade to a newer version of ControlST.

- **Minimize the impact of switch operating system changes**: network switch vendors periodically update the switch operating systems, and in some cases these changes have required ControlST updates to support new behaviors that were introduced as part of the operating system update. The switch layout files have been designed to minimize the impact of internal switch layout changes. In the event that internal switch changes cannot be supported by an existing switch layout, a new switch layout will be included in the next ControlST release. A new layout file can be requested to provide the ability to import the new switch layout into the site’s existing ControlST version. Refer to the table *Network Switch Layout Version Compatibility* for a complete version compatibility list.

- **Support for unqualified (custom) switch types**: GE standard switch layouts are provided for all NetworkST standard switch configurations. Support for non-standard switch types can be added by creating custom layout files.

### Network Switch Layout Version Compatibility

<table>
<thead>
<tr>
<th>ControlST Version</th>
<th>Single-product Release Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>V07.04.05C SP04 (and higher within V07.04 branch)</td>
<td>ToolboxST V07.04.09C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.04.09C and higher</td>
</tr>
<tr>
<td>V07.05.00C SP01 (and higher within V07.05 branch)</td>
<td>ToolboxST V07.05.01C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.05.01C and higher</td>
</tr>
<tr>
<td>V07.06.00C and higher</td>
<td>ToolboxST V07.06.00C and higher</td>
</tr>
<tr>
<td></td>
<td>WorkstationST V07.06.00C and higher</td>
</tr>
</tbody>
</table>
4.3.1 Configure Switch Layouts for New Sites

When configuring a new system with a ControlST version that supports the Network switch Layout feature (refer to the table *Network Switch Layout Version Compatibility*), only the GE standard switch layouts are available by default. The GE standard switch layouts correspond to the standard switch types supported by NetworkST. The following figure displays the switch device Switch Layout Type property with the list of available switch layout types.

*Note*  Layouts for GE standard NetworkST switch types always begin with GE, followed by the switch manufacturer, model number, and any model-specific options (GE_<Manufacturer>_<Model>_<Options>).

The GE standard switch layouts support any NetworkST qualified Cisco® switch. Switches from other manufacturers have been supported on a legacy basis but it is not anticipated that these switches will be used often in new systems. If support for a legacy switch type is required on a new system, legacy switch support can be enabled using the following procedure.
➢ To enable legacy switch support on a new system

1. From the System Information Editor Tree View, select Network Switch Layouts to display the supported switch layouts.

2. From the Property Editor, set the Enable Legacy Switch Support property to True to display the legacy switch layouts.
When this setting is enabled (True), the legacy switch types are available for selection when modifying the network switch configuration, as shown in the following figure.

Note: Always use the GE standard switch layouts when available. For example, always use the GE_CISCO_2960_24Port layout but never use the legacy Cisco_Catalyst_2960 layout. In the case where a supported legacy switch such as the Enterasys_N1 is required, the legacy layout must be used because there are no GE standard layouts defined for Enterasys switches.

Refer to section Custom Network Switch Layout Configuration for the procedure to create custom switch layouts. For example, the GE standard switch layouts only support 24 port versions of the Cisco 2960 switch. Support for a 48 port Cisco 2960 switch is not available with the GE standard layouts, but a custom switch layout can be created to allow monitoring of this non-standard switch type.

Note: The custom layout is used for qualifying new switch types and cannot be used for normal operation. The switch is not monitored when the custom layout is selected.
4.3.2 Manage Switch Layouts when Upgrading Existing Sites

When a system that was created by an older version of ControlST is opened in ToolboxST V07.05.01C or later, the legacy switch support is enabled by default, and the existing switch configurations remain valid without opening or building the existing switch configurations. Although it is not necessary to upgrade the switch configurations, the best practice is to upgrade any Cisco switches to the GE qualified layout if one is available. For example, a switch configured for the legacy Cisco_Catalyst_2960 layout should be updated to use the GE_CISCO_2960_24Port layout. Updating the switches to the GE qualified switch layouts will insulate the site against future switch operating system changes that are most likely to occur if a switch fails and is replaced with a newer version.

Attention

Whenever a GE standard switch layout is selected for a switch type that supports stacking, stacking is enabled by default and the number of switches in the stack is initialized to the maximum stack size defined by the switch layout type. Do not forget to modify these properties to match the actual layout of the switch being configured.
4.3.3 Add Support for Newly Qualified NetworkST Standard Switch Types

New GE standard switch layouts are created as new switch types are qualified for NetworkST. The new standard switch layouts are added to the GeSwitchLayouts.xml file, which is then used to update older versions of ControlST with the latest standard switch layouts. Any ControlST version that supports the GE standard switch layouts (V07.05.01C and later) can be updated to support the latest GE standard switch layouts by updating the GeSwitchLayouts.xml file. Simply copy the latest GeSwitchLayouts.xml file to the top level of the ToolboxST project directory (the directory where the .tcw file is located), then close ToolboxST and re-open the project to make the new GE standard switch layouts available.

Note For systems under CMS source control, first check out the system configuration (check out from the root tree node of the system overview), then copy the new GeSwitchLayouts.xml file in place of the existing one. Open the System Information Editor by double clicking on the system overview root tree node. Make some change to something in the editor and change it back so the document requires saving. Save the editor and close it. Check the system back into CMS.

4.3.4 Custom Network Switch Layout Configuration

The Network Switch Layouts in ToolboxST provide the mapping between the internal switch interfaces and the physical switch ports, which enables the CSH feature to read the switch data over SNMP and display the data with the correct physical port location.

ToolboxST provides GE standard switch layouts that correspond to all supported NetworkST standard switch types. Support for non-standard switch types can be configured by creating custom Network Switch Layouts, which are used to enable the CSH to monitor non-standard switch types.

Note The use of a non-standard switch implies that the user assumes responsibility for all aspects of the switch configuration and its interaction with and impact on the network. Switch configuration is beyond the scope of this document. SNMP V1 or SNMP V3 must be enabled and properly configured in the switch to enable monitoring of the switch values.

Network Switch Layouts allow users to enter unique physical port-to-port faceplate and interface name mapping. The Network Switch Layouts include a set of legacy switch layout types that were supported before the ability to add custom switch layouts existed. These legacy switch layout types cannot be edited, but are presented for completeness and to allow easy version upgrade. There is also a set of GE standard switch layout definitions that cannot be modified but are included as validated switch layouts.
➢ To add a custom Network Switch Layout

1. From the System Information Editor, expand the Network Switch Layouts.

2. From the Tree View of layouts, right click a port, select Add Switch Layout, and enter a unique name for the layout. (As an alternative, you may copy an existing one.)

3. From the Property Editor, modify the properties to configure the switch layout.
## Network Switch Layout Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Is a legacy layout</td>
<td>Legacy layouts; cannot be modified (False)</td>
</tr>
<tr>
<td>Is Stackable</td>
<td>Switch is a stackable switch (default is True)</td>
</tr>
<tr>
<td>Maximum Stack Size</td>
<td>Maximum number of stacked switches allowed. This setting limits the Stacked Switch Group Size setting in the Network Switch component editor.</td>
</tr>
<tr>
<td>Number of ports on each switch</td>
<td>Sets the number of ports on each switch. For a stacked switch this number controls how many ports are defined as the Stacked Switch Group Size is set. For a non-stacked switch this controls the total number of ports. For the switch layout, all ports are shown per the Maximum Stack Size and Ports Per Switch setting.</td>
</tr>
<tr>
<td>Standard Layout</td>
<td>Standard GE switch configurations are part of the product. This switch layout is a standard configuration; cannot be modified (False).</td>
</tr>
<tr>
<td>Switch Layout Type</td>
<td>Name of the type of switch. There are some pre-defined legacy switch types that were used by previous ToolboxST / WorkstationST versions, which are included but cannot be modified.</td>
</tr>
<tr>
<td>Switch Manufacturer</td>
<td>Manufacturer of the network switch. There are some manufacturers that require special SNMP behavior by the WorkstationST Network Monitor.</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Supports Dual Power Supplies</td>
<td>True if the switch type provides standard redundant power supply connections that can be optionally connected to a power source for Simplex or redundant power supply operation.</td>
</tr>
<tr>
<td>Supports Fan Monitoring</td>
<td>True if the switch type has internal fans and provides the ability to monitor them via SNMP.</td>
</tr>
<tr>
<td>Supports Power Supply Monitoring</td>
<td>True if the switch type provides the ability to monitor the switch power supplies via SNMP.</td>
</tr>
<tr>
<td>Supports Temperature Monitoring</td>
<td>True if the switch type has internal temperature sensors and provides the ability to monitor them via SNMP.</td>
</tr>
</tbody>
</table>

In the Data Grid View, each non-legacy switch allows modification to port information.

<table>
<thead>
<tr>
<th>Port Location</th>
<th>Faceplate Port Number</th>
<th>Faceplate Port Name</th>
<th>Port Number</th>
<th>Faceplate Port Port Text</th>
<th>Interface Name</th>
<th>Stack Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 001 X</td>
<td>1</td>
<td>Port</td>
<td>1</td>
<td>X</td>
<td>FastEthernet1/1</td>
<td>1</td>
</tr>
<tr>
<td>Port 002 X</td>
<td>2</td>
<td>Port</td>
<td>2</td>
<td>X</td>
<td>FastEthernet1/2</td>
<td>1</td>
</tr>
<tr>
<td>Port 003 X</td>
<td>3</td>
<td>Port</td>
<td>3</td>
<td>X</td>
<td>FastEthernet1/3</td>
<td>1</td>
</tr>
<tr>
<td>Port 004 X</td>
<td>4</td>
<td>Port</td>
<td>4</td>
<td>X</td>
<td>FastEthernet1/4</td>
<td>1</td>
</tr>
<tr>
<td>Port 005 X</td>
<td>5</td>
<td>Port</td>
<td>5</td>
<td>X</td>
<td>FastEthernet1/5</td>
<td>1</td>
</tr>
<tr>
<td>Port 006 X</td>
<td>6</td>
<td>Port</td>
<td>6</td>
<td>X</td>
<td>FastEthernet1/6</td>
<td>1</td>
</tr>
<tr>
<td>Port 007 X</td>
<td>7</td>
<td>Port</td>
<td>7</td>
<td>X</td>
<td>FastEthernet1/7</td>
<td>1</td>
</tr>
<tr>
<td>Port 008 X</td>
<td>8</td>
<td>Port</td>
<td>8</td>
<td>X</td>
<td>FastEthernet1/8</td>
<td>1</td>
</tr>
<tr>
<td>Port 001</td>
<td>1</td>
<td>Port</td>
<td>9</td>
<td></td>
<td>GigabitEthernet1/1</td>
<td>1</td>
</tr>
<tr>
<td>Port 002</td>
<td>2</td>
<td>Port</td>
<td>10</td>
<td></td>
<td>GigabitEthernet1/2</td>
<td>1</td>
</tr>
</tbody>
</table>
### Switch Layout Data Grid Column Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Location</td>
<td>Read only indication of the stack and face plate port number</td>
</tr>
<tr>
<td>Faceplate Port Number</td>
<td>Port number on the switch nameplate. This number is the same on all individual switch ports for a stacked switch, but the Stack Number will be different.</td>
</tr>
<tr>
<td>Faceplate Port Name</td>
<td>Faceplate port name. This is used in the port location which is displayed in the network status viewer.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number returned from SNMP queries and shown using the switch command line interface</td>
</tr>
<tr>
<td>Faceplate Port Text</td>
<td>Text is appended after the port number into the Port Location field</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Interface name that can be viewed through the switch command line interface (for example, FastEthernet1/4)</td>
</tr>
<tr>
<td>Stack Number</td>
<td>Stack number for a stackable switch (1 for a switch that does not support stacking)</td>
</tr>
</tbody>
</table>
4.4 Switch Stacking and Hardware Monitoring

Beginning with ControlST V07.07.00C, CSH monitors the health of the stack members for stacked switch configurations, as well as the hardware status for stand-alone switches and individual switch stack members.

4.4.1 Switch Stack Monitoring

Switch stacking is used to make multiple switches behave as a single switch. Switch types that support stacking can normally be configured for either stand-alone or stacked mode. CSH monitors the stack health of any switch of a type that supports stacking and is configured for stacking mode.

Stack Provisioning Health Monitoring

Stack provisioning reflects the number of switches a stack is configured to support. CSH monitors the configured stack size and the switch stack provisioned capacity in order to provide an indication if the switch configuration in ToolboxST exceeds the capacity of the actual switch stack. CSH requests the stack configuration from the switch and compares the number of provisioned switches with the stack size configured for the switch in ToolboxST. CSH reports errors if the stack size configured in ToolboxST exceeds the provisioned capabilities of the switch. Provisioning errors are addressed by either modifying the switch configuration in ToolboxST to a stack size supported by the switch stack, or by increasing the provisioned size of the switch stack.

CSH also monitors the status of each stack member and reports errors if a stack member is not actively participating in the stack.

In the example displayed in the following figure, the switch is configured as a stack with two stack members, each with 12 ports per switch.

![Example Switch Stack ToolboxST Configuration](image)

CSH reads the provisioned status from the switch and reports it in the CSH Viewer, as illustrated in the following figure.

![Example Switch Stack Provision Status in CSH Viewer](image)
The switch stack provision status is also displayed as part of the tooltip information for the switch in the Network Status Viewer.

Example Switch Stack Provision Status in Network Status Viewer

In the example displayed in the following figure, the stack size configured in ToolboxST exceeds the provisioning of the switch.

Example Switch Stack Exceeds Switch Provisioning ToolboxST Configuration
The CSH Viewer indicates the error as shown in the following figure.

**Example Switch Stack Provision Errors in CSH Viewer**

CSH generates provisioning alarms that can be viewed from the Diagnostics tab, as well as in the WorkstationST Alarm Viewer.

**Example Switch Stack Provision Errors on Diagnostics Tab in CSH Viewer**
The switch stack provision error is also displayed as part of the switch status text and as part of the tooltip information for the switch in the Network Status Viewer.
Stack Member Health Monitoring

CSH monitors the status of each stack member and reports errors if a stack member is not actively participating in the stack. In the example displayed in the following figure, the switch is configured with a stack size of four.

![Example Switch Stack Member ToolboxST Configuration](image1)

The actual switch is provisioned for four stack members, but in this example there are only two physical switches currently in the stack, and the switch reports these **missing** switches with a **Provisioned/Not Ready** status. Any status other than **Ready** indicates that the switch is not participating in the stack. The CSH Viewer reports the error condition and shows status of each stack member. Note that if you hover over the **Switch Stack Status Info** field, the stack member data is displayed in table format as shown in the following figure.

![Example Switch Stack Member Status in CSH Viewer](image2)
The stack member status for the individual Stack Members is also displayed at the Stack Member level in the CSH Viewer.

Example Switch Stack Status at Member Level in CSH Viewer

CSH generates Stack Member alarms that can be viewed from the Diagnostics tab, as well as in the WorkstationST Alarm Viewer.

Example Stack Status Errors on Diagnostics Tab in CSH Viewer
The switch stack member status is displayed as part of the tooltip information for the switch in the Network Status Viewer.
4.4.2 Hardware Monitoring: Power Supplies

CSH can be configured to monitor the status of the switch power supplies. The Monitor Power Supplies property is available in the switch configuration for switch types that support this capability. In the following figure, power supply monitoring has been enabled (Monitor Power Supplies property is set to True).

![Power Supply Monitoring ToolboxST Configuration](image)

CSH automatically monitors the status of all of the internal power supplies of the switch. In this example, the selected stack member has two internal power supplies and they are both operating without any errors, which can be viewed from the Status tab in the CSH Viewer as shown in the following figure.

![Example Switch Internal Power Supply Status in CSH Viewer](image)
The status of the switch power supplies is also displayed as part of the tooltip information for the switch in the Network Status Viewer.

Example Switch Internal Power Supply Status in Network Status Viewer
Unplugging the AC power cord from one of the power supplies generates a power supply error that is reported on the Status tab, and generates an alarm that can be viewed from the Diagnostics tab.

**Example Power Supply Error on Status Tab in CSH Viewer**

**Example Power Supply Error on Diagnostics Tab in CSH Viewer**
The switch power supply error is also displayed in the switch tooltip information in the Network Status Viewer.

**Note** CSH automatically monitors all power supplies in the switch. Some switch chassis have slots that accept power supply modules and therefore allow the capability for single or redundant power supplies. Any power supply modules that are installed but do not have AC power connected to them will be reported as a failed power supply because it is assumed that there is no good reason to add the expense of a redundant power supply module but not provide power to it. If power redundancy is not desired, unplug the redundant power supply modules from the switch to avoid redundant power supply errors.
Dual Power Supply Example

Some switch types (primarily the Cisco IE2000 switches) come with internal dual power supplies, and power can optionally be connected to either one of them for non-redundant power or to both of them for redundant power.

The switch device configuration in ToolboxST provides the properties to support any combination of power connections to the switch, as displayed in the following figure.

Configure the Monitoring properties, Power Supply 1 Connected and Power Supply 2 Connected, to report errors or alarms only for the connected (used) power supplies as follows:

➢ To configure dual power supplies to report errors or alarms for connected power supplies only
   • If only DC-A is connected to a power source, set Power Supply 1 Connected to True and set Power Supply 2 Connected to False.
   • If only DC-B is connected to a power source, set Power Supply 1 Connected to False and set Power Supply 2 Connected to True.
   • If both DC-A and DC-B power connections are connected to a power source, set both Power Supply 1 Connected and Power Supply 2 Connected to True.
4.4.3 Hardware Monitoring: Fans

CSH can be configured to monitor the status of the internal switch fans. The Monitor Fans property is available in the switch configuration for switch types that support this capability. In the example displayed in the following figure, Fan Monitoring has been enabled (Monitor Fans property is set to True).

![Switch Internal Fan Monitoring ToolboxST Configuration]

CSH automatically monitors the status of all of the internal switch fans. In the example displayed in the following figure, the selected stack member has two internal fans and they are both operating without any errors. This can be viewed in the CSH Viewer from the Status tab as shown in the following figure.

![Example Switch Internal Fan Status in CSH Viewer]
The switch fan status is also displayed in the switch tooltip information in the Network Status Viewer.

![Example Switch Fan Status in Network Status Viewer](image)

Internal fan failures are reported as an error and an alarm will be generated. The CSH Viewer displays these errors in the Diagnostics tab, as shown in the following figure.

![Example Internal Fan Error on Diagnostics Tab in CSH Viewer](image)
The switch fan error is also displayed in the switch tooltip information in the Network Status Viewer.

Example Switch Fan Status in Network Status Viewer
4.4.4 Hardware Monitoring: Temperature Sensors

CSH can be configured to monitor the status of the internal switch temperature sensors. The Monitor Temperature property is available in the switch configuration for switch types that support this capability. In the example displayed in the following figure, temperature sensor monitoring has been enabled (Monitor Temperature property is set to True).

![Switch Internal Temperature Monitoring ToolboxST Configuration](image)

CSH automatically monitors the status of all of the internal switch temperature sensors. In the example displayed in the following figure, the selected stack member has one internal temperature sensor that is reporting temperature in the normal range, which can be viewed from the CSH Viewer Status tab.

![Example Switch Internal Temperature Status in CSH Viewer](image)

The switch temperature sensor status is also displayed in the switch tooltip information in the Network Status Viewer.
Example Switch Internal Temperature Status in Network Status Viewer

Switches with Temperature Sensor readings that exceed normal values will indicate an error in the tooltip information in the Network Status Viewer, and an alarm will be generated.
4.5 Configure Local HMI Management Address

As the system overview shows, the workstations do not have direct access to the management network, and communications with the network switches can only occur through network routing between the PDH network and the management network (MGH). The network router is typically configured to allow only PDH traffic from a single IP address. The CSH feature must be configured to send all requests to the network switches over the PDH network using this established PDH address as the source address of the request. The Local HMI Management Address property of the CSH feature is used to specify this predefined management network routable PDH address. Typically this address will be configured as 172.16.201.60.

➢ To configure the CSH feature: From the Tree View, double-click the WorkstationST item to display the Component Editor.

![Diagram showing configuration steps for CSH feature]
4.6 **Add Local HMI Management Address to PDH Adapter in Workstation**

The Local HMI Management Address must be added to the PDH (plant scope) network adapter of the computer running the CSH.
5 Configure Local HMI Management Address for Systems without Switch Management Network

To increase the security of the network infrastructure, the network switches are being configured with restricted access to the switch SNMP data. The CSH feature must be configured correctly to gain access to the switch SNMP data. Without this SNMP data, the switch information such as port status and connected devices will be unknown. This causes the CSH to generate Topology Error alarms for all of the devices in the system, and preventing the CSH from detecting network issues.

5.1 Configure Local HMI Management Address in CSH Feature

Updated switch configurations include an Access Control List (ACL) that blocks all SNMP data requests except for those from a single, predefined IP address, which is referred to as the Local HMI Management Address. In order to get SNMP data from the network switches, the Network Monitor must send all SNMP requests with the Local HMI Management Address as the source address in the TCP/IP message header. The Local HMI Management Address property of the Network Monitor feature is used to specify this address, which is typically configured as 172.16.201.60 in the network switches.

➢ To configure the Local HMI Management Address: From the Tree View, double-click the WorkstationST item to display the Component Editor.
5.2 Add Local HMI Management Address to PDH Adapter in Workstation

The Local HMI Management Address must be added to the PDH (plant scope) network adapter of the PC running the CSH feature.
6 Network Switch SNMP Configuration

CSH uses Simple Network Management Protocol (SNMP) to read data from the network switches to determine the state of the switch ports, which devices are connected to them, and so forth. In previous releases, CSH and the network switches only implemented the SNMP V1 protocol. As a security enhancement, ControlST and the network switches have been expanded to use the SNMP V3 protocol, which introduces strong authentication and data encryption to securely read data from the network switches. ControlST V07.02.00C SP01 and earlier versions use the SNMP V1 protocol to read SNMP data from the network switches. ControlST V07.02.00C SP02 and later versions can use either the SNMP V1 or SNMP V3 protocol to read data from the network switches.

**Network Switch SNMP Protocol Version Compatibility**

<table>
<thead>
<tr>
<th>Application</th>
<th>SNMP V1 Protocol</th>
<th>SNMP V3 Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlST</td>
<td>ControlST V07.02.00C SP01 and earlier</td>
<td>ControlST V07.02.00C SP02 and later</td>
</tr>
<tr>
<td>NetworkST</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

6.1 New System Configuration

The SNMP Mode and security information is configured and displayed from the WorkstationST Network Monitor configuration tab, located under the Network Monitor Data Acquisition property group.

The following figure displays the properties that are listed when SNMP Mode V1 is selected.

![SNMP V1 Mode Properties](image)

The following figure displays the properties that are listed when SNMP Mode V3 is selected.
6.1.1 SNMP V1 Configuration

➢➢

1. Open the appropriate .tcw system file and double-click the WorkstationST device to open the WorkstationST Component Editor.
2. Select the Control System Health tab to display the SNMP Mode and security information located under the Network Monitor Data Acquisition property group.
3. From the SNMP Mode drop-down menu, select V1.
4. Click the SNMP V1 Community property Edit button to display the Change Password dialog box.
5. Enter the SNMP V1 Community name in the New Password field, re-enter it in the Verify Password field, and click OK to save it.
6. Perform a **Build, Download** to the WorkstationST device to save the configuration, and restart the CSH feature to display the new configuration values.

**Tip** You can verify the configured SNMP Mode and the SNMP V1 Community Name used by the CSH feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security information in the tooltip. The Community Name is hidden for security.

![Configured SNMP V1 Mode and Community Name Displayed in Network Status Viewer](image)

**Note** Refer to the chapter *Troubleshoot Network Switch SNMP Issues* for assistance with resolving SNMP configuration issues.
6.1.2 SNMP V3 Configuration

➢➢ To configure SNMP V3 Mode

1. Open the appropriate .tcw system file and double-click the WorkstationST device to open the WorkstationST Component Editor.

2. Select the Control System Health tab to display the SNMP Mode and security information located under the Network Monitor Data Acquisition property group.

3. From the SNMP Mode drop-down menu, select V3.

![Network Monitor Data Acquisition](image)

4. Click the SNMP V3 Authentication Password property Edit button to display the Change Password dialog box.

![Change Password](image)

5. Enter the SNMP V3 Authentication password in the New Password field, re-enter it in the Verify Password field, and click OK to save it.

6. Click the SNMP V3 Encryption Password property Edit button to display the Change Password dialog box.
7. Enter the SNMP V3 Encryption password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password](image)

8. Enter the SNMP V3 user name for the **SNMP V3 User Name** property.

![Network Monitor Data Acquisition](image)

9. Perform a **Build, Download** to the WorkstationST device to save the configuration, and restart the CSH feature to display the new configuration values.

**Tip** You can verify the configured SNMP Mode and security settings used by the CSH feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security settings in the tool tip. The Authentication and Encryption Password values are hidden for security.
Configured SNMP V3 Mode and Security Settings Displayed in Network Status Viewer

Note Refer to the chapter Troubleshoot Network Switch SNMP Issues for assistance with resolving SNMP configuration issues.

6.1.3 Network Switch SNMP Override Settings

The SNMP configuration settings are typically configured the same for all of the network switches at the site. When this is the case, the SNMP settings on the configuration tab specify the SNMP settings for all of the network switches in the system. Situations may arise where different SNMP configurations are needed between network switches. For example, a site may replace a failed switch that only supports SNMP V1 (ControlST V07.02.00C SP01 and earlier versions) with a new switch with SNMP V3 support (ControlST V07.02.00C SP02 and later). In this case, the site may choose to enable SNMP V3 protocol to collect data from the new switch while leaving the existing switches at SNMP V1 protocol. ToolboxST provides network switch device override settings to override the CSH feature-level settings.

➢ To enable the local SNMP Parameter Override property

1. Open the appropriate .tcw system file and double-click the Network Switch device to open the Network Switch Component Editor.

The SNMP Parameter Override settings are located under the SNMP Overrides property group.
2. From the **SNMP Local Parameter Override** drop-down menu, select **True**. When set to True, the locally configured SNMP settings are used instead of the SNMP settings configured at the CSH feature level.

3. From the **SNMP Mode** drop-down menu, select the appropriate value as V1 or V3.
   a. If SNMP Mode V1 is selected, perform the following steps:
      i. Click the **SNMP V1 Community Name** property **Edit** button to display the **Change Password** dialog box.
ii. Enter the SNMP V1 Community name in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password dialog box]

b. If SNMP Mode **V3** is selected, perform the following steps:

i. Enter the SNMP V3 user name for the **SNMP V3 User Name** property.

![SNMP Overrides](image)

ii. Click the **SNMP V3 Authentication Password** property **Edit** button to display the **Change Password** dialog box.

![Change Password dialog box](image)

iii. Enter the SNMP V3 Authentication password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.
iv. Click the **SNMP V3 Encryption Password** property **Edit** button to display the **Change Password** dialog box.

![SNMP V3 Encryption Password](image)

v. Enter the SNMP V3 Encryption password in the **New Password** field, re-enter it in the **Verify Password** field, and click **OK** to save it.

![Change Password Dialog](image)

4. Perform a **Build** to build the switch device, save the configuration, and automatically restart the CSH feature to display the new configuration values.

**Tip** You can verify the configured SNMP Mode and security settings used by the CSH feature from the Network Status Viewer. With your cursor, hover over each network switch to display the SNMP Mode and security settings in the tool tip. The SNMP V1 Community Name and the SNMP V3 Authentication and Encryption Password values are hidden for security.

![Network Status Viewer](image)

**Configured SNMP V3 Mode and Security Settings Displayed in Network Status Viewer**
➢ To disable the local SNMP Parameter Override property

1. Open the appropriate .tcw system file and double-click the Network Switch device to open the Network Switch Component Editor.

2. From the SNMP Local Parameter Override drop-down menu, select False.

3. Perform a Build to build the switch device, save the configuration, and automatically restart the Network Monitor feature to display the new configuration values.
6.2 ControlST Upgrade

ControlST V07.02.00C SP01 and earlier versions only support the SNMP V1 protocol to read data from the network switches. The only required SNMP setting was the SNMP Community name, which was configured at the switch level as shown in the following figure.

When upgrading from ControlST V07.02.00C SP01 or earlier versions to a newer version that supports SNMP V3 settings (ControlST V07.02.00C SP02 and later), the network switch device in ToolboxST automatically captures the SNMP V1 switch configuration settings and updates them with the new settings: the SNMP Local Parameter Override property is set to True, the SNMP Mode is set to V1, and the SNMP Community is copied to the SNMP V1 Community Name property of the switch device. The changes are saved and permanently stored when the switch device is built after upgrade. This allows the SNMP V1 settings to continue to be managed at the switch level after a ControlST upgrade without the user having to make any changes to the network switch configuration. The following figure displays the switch SNMP settings after a ControlST upgrade has been performed.
After the upgrade is complete, promote management of the switch SNMP parameters to the CSH feature level by configuring the feature-level SNMP settings and clearing the SNMP Local Parameter Override setting, then perform a build of each network switch.

### 6.3 Network Switch Replacement (Upgrade)

The default network switch configuration from the factory supports both SNMP V1 and SNMP V3 protocols. The following options are available when replacing a network switch that only supports the SNMP V1 protocol with a network switch that supports the SNMP V3 protocol:

- **Continue using SNMP V1:** configure the replacement network switch in the same way as the replaced switch. This is the only option in a system using ControlST V07.02.00C SP01 or earlier versions that only support the SNMP V1 protocol. The default switch configuration supports both SNMP V1 and SNMP V3 protocols. Modify the ToolboxST network switch device’s Management IP Address to match the IP address of the replacement switch, and configure the switch’s SNMP Community to match the replaced switch’s Community Name. Build the switch device to update the configuration and restart the CSH feature with the new values.

- **Configure the ToolboxST network switch device for SNMP V3:** update the ToolboxST switch device configuration to benefit from the SNMP V3 capability of the replacement switch. This option is only available if the system in which the switch is being implemented has ControlST V07.02.00C SP02 or later with SNMP V3 support. Set the ToolboxST switch device SNMP Local Parameter Override to True, set the SNMP Mode to V3, and set the SNMP V3 User Name, SNMP V3 Authentication and Encryption passwords to match the network switch configuration. Build the switch device to update the configuration and restart the CSH feature with the new values.
7 Control Server Support

The term Control Server refers to a collection of Virtualization Servers (referred to as the Server Set) and the Virtual Machines (VMs) that are hosted by them. The CSH feature collects health data for the Control Server components, publishes these values to the system OPC UA server, and generates alarms when error conditions are detected.

The Control System Health Viewer provides a read-only view of real-time data and a filtered view of alarms based on the selected component.

The key benefits of Control Server monitoring in the CSH include:

- Read-only, simplified status information
- Integrated alarms
- Instant notification of issues
- Rapid navigation to the source of issues
- OPC UA values can be consumed by operator screens and third-party applications
- Status Data Trending

7.1 Control Server Monitoring Overview

vSphere is the brand name for VMware’s virtualization products that includes the ESXi hypervisor and the suite of monitoring software, such as vCenter and the vSphere Client application. Control Server is built upon the vSphere platform. The vSphere monitoring tools are extremely comprehensive and powerful, making them very difficult to understand and dangerous when used by untrained or inexperienced users.

The CSH feature addresses this issue by collecting key health data from vSphere and presenting it in a simplified, read-only, system health focused view. This allows users without any knowledge of the vSphere platform to make a rapid assessment of the Control Server health with no danger of making unintentional changes to the system. CSH also generates alarms that provide a complete description of any detected failure modes. The simplified health view and user-friendly alarms make detecting issues and identifying the source of issues simple, without the need for any vSphere knowledge of the underlying hypervisor platform.

7.1.1 Control System Health Viewer

Control Server health information is displayed beneath the Virtualization Platform node of the Control System Health Viewer. The Control System Health Viewer provides a hierarchical view of the servers that make up a Control Server Set and the VMs hosted by them. This view is similar to the view provided by the VMware vSphere Web Client, with a focus on critical health information that facilitates immediate determination of the overall health of all of the server sets and rapid discovery of hardware and system issues.
vCenter View of HA Control Server with Corresponding CSH View

CSH generates alarms that are forwarded to the system Alarm Server when error conditions are detected. These alarms can be viewed from the Diagnostics tab of the Control System Health Viewer, as well as from the system Alarm Viewer.
Refer to the section [Virtualization Platform Health Information](#) for more detailed information.

### 7.1.2 Trender

All of the Control Server health data generated by CSH is published to the system OPC UA Server, making it available for display in the Toolbox Trender and other third-party OPC UA Clients.

Refer to [Appendix F Trending Control System Health Data Example](#) for more information.
7.2 Control Server Configuration Overview

The Control Server components are configured using the ToolboxST application. The CSH feature uses this information to recognize the components, along with the information required to monitor them.

The virtualization servers and the VMs hosted by them are added to the ControlST system using ToolboxST. With the exception of the Workstation VMs, all virtualization components in ToolboxST are placeholders for the Virtualization servers and VMs running in the Virtualization Server Set. These components provide the template for the expected Control Server topology without affecting the actual configuration of these components. This is exactly the way the network switch devices are represented in the system. The networks switch devices in ToolboxST reflect the aspects of the switch that must be known by CSH to monitor them (such as IP address and SNMP community name) and also provides the mechanism to define which devices are connected to the switch ports so that they can be monitored by the CSH.

The following figure displays the VMware vSphere Web Client view for an HA Control Server next to the view of the server set, servers, and VMs for the same system configured in ToolboxST.
8 Thin Client HMI Support

Thin Client HMI involves replacing standalone HMI PCs (also referred to as Thick Clients) with a centralized server running Virtual Machines, which are accessed using Thin Client terminals at the different plant locations. This section explains how to configure the ControlST system to allow the Network Monitor Server / Network Monitor to monitor the Server and Thin Client terminals connected to the Network Switches. The steps to configure the system for HMI Thin Client support are:

1. Create an HMI Server group to provide a location to collect all of the Workstations in the system that are running as Virtual Machines on the server.
2. Set the Virtualized property for each Workstation running as a Virtual Machine on the server.
3. Configure the Network Switch ports connected to the Server.
4. Configure the Network Switch ports connected to the Thin Client terminals.

8.1 Create HMI Server Group

➢➢ To create an HMI Server group

1. From the ToolboxST System Editor Tree View, right-click the system icon, select Insert New and Group from the drop-down menus, and enter a Name (HMI Server) for the group.
2. From the **Tree View**, right-click the new group (**HMI Server**) icon, select **Insert New** and **WorkstationST** from the drop-down menus, and enter a **Name (Wkstn1)** for the workstation. (Repeat this step for each of the Thin Client workstations to be added to the system.)
8.2 Configure Workstations Running as Virtual Machines

➢ To set the Virtualized property for each workstation

1. From the Tree View, double-click a workstation in the new group to display the WorkstationST Component Editor.
2. From the Property Editor, select Visualized and set it to True.

3. Repeat this procedure for each of the workstations in the group.
8.3 Configure Network Switch Ports Connected to Server

➢ To configure the network switch ports

1. From the ToolboxST System Editor Tree View, double-click the network switch (General) to display the Component Editor.

2. From the Summary View, for each Port to be connected to the server, select Port Connection, set it to Server, select Port Description and enter a detailed description for ease of identification. This description will be displayed in the Network Status Viewer and will be included in any alarms generated for the port.

![Network Switch Port Configuration](image-url)
8.4 Configure Network Switch Ports Connected to Thin Client Terminals

➢ To configure the network switch ports

1. From the ToolboxST System Editor Tree View, double-click the network switch (General) to display the Component Editor.

2. From the Summary View, for each Port to be connected to the Thin Client workstation, select Port Connection, set it to Thin Client, select Port Description and enter a detailed description for ease of identification. This description will be displayed in the Network Status Viewer and will be included in any alarms generated for the port.
8.5 Server and Thin Client Terminal Alarms

Alarms associated with the Server and Thin Client terminal network switch ports are automatically generated based on the network switch port configurations. The following figures show the port configurations with descriptions and shows the corresponding alarms, which include the configured port descriptions.
9 Control Server Configuration

The Control Server components and the VMs that it hosts must be configured in ToolboxST to allow the CSH feature to monitor them.

9.1 Add New Control Server

The following steps provide a high-level overview of the process to add a new Control Server to the system configuration, followed by a detailed procedure.

1. Insert a new Control Server set component.
2. Provide a name for the Control Server component.
3. Select a HA or Simplex template to use as the starting point for the Control Server set configuration.
4. Add and/or remove the virtualization servers and VMs to reflect the appropriate Control Server topology.
5. Save the changes to automatically add the specified devices to the system configuration.

➢➢ To add a new Control Server

1. From the ToolboxST main menu, select Edit, Insert New, Control Server, and Control Server Set to display the Control Server Creation Wizard.
2. Enter the name of the Control Server and click **Next**.
3. Select a High Availability or Simplex template to use as the starting point for the Control Server set configuration, then click **Next**.
The Control Server Creation Wizard displays the Control Server components based on the selected template. The default High Availability and Simplex templates provide the starting point for a typical Control Server configuration. Custom templates can be created in the System Information Editor.
4. Select a component to display the configuration properties in the Property Editor (right side of the window). The following figure displays the server set properties. Edit the default properties in the Property Editor or from the Control Server Component Editor. Refer to the section Virtualization Server Set Configuration for more information on configuring these properties.
5. Add or remove Control Server and VM components as follows:
   a. To delete a component, select and right-click the component, then select **Delete**.
   b. To add a component, perform the following steps:
      i. Select the destination (either the cluster or one of the virtualization servers), right-click, and select **Add**.

   **Note** In an HA server set, VM components (which includes the VM, Virtual Field Agent, and WorkstationST VM) can be added to the cluster or to a specific Virtualization server. VMs added to the cluster represent VMs that can migrate between the servers using the HA feature. VMs added to a specific server represent VMs that do not participate with the HA feature and only run on the specified server.

   ii. Enter the device name and select the appropriate device type from the drop-down menu.

   iii. Click **OK** to add the new VM to the server set.

   iv. Select the new VM and configure its properties in the Property Editor.
c. Repeat these steps to add additional VMs to the server set.
6. Click **Finish** to save the changes and add the virtualization servers and VMs to the system configuration (refer to the following figure for an example).
It is recommended to create a Group with the same name as the Control Server set that can be used as a container for all of the server set’s components and move all of the virtual components associated with the server set within the Group as shown in the following figure.

![Example Control Server Set Group](image)

After the virtual components have been added to the system, they must be individually configured and built. Refer to the following sections for the procedures to configure the different virtual component types.
9.2 Add Components to Existing Control Server

The following steps provide a high-level overview of the process to add a component to a Virtualization Server Set after it has been created using the Control Server Creation Wizard, followed by a detailed procedure.

1. Create a new component.

2. (Optional) Move the component into the Control Server’s Group.

3. Add a corresponding child device to the Virtualization Server Set configuration.

Note A child device can be added to the Virtualization Server Set before it is created and added to the system configuration; however, attempts to build the Virtualization Server Set will fail with an error such as follows until the device is created.

➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢➢ geli
2. Enter the name of the VM and click **Finish**.

3. The TestVM device displays in the Summary View. Select the TestVM device and drag it to the Control Server Group as illustrated in the following figure.

4. Open the TestVM device and configure and build it. Refer to section **Virtual Machine Configuration**.

5. Open the Virtualization Server Set device and expand the Virtualization Server Tree View item. For this example, the server set is configured for High Availability.
6. Right-click on the Cluster node and select **Add** to add the VM to Cluster to indicate that it can migrate between servers.

7. Enter the device name and device type and click **OK**.
The TestVM is added to the Virtualization Server Set.

8. Build the server set to save the changes and update the system configuration server.
9.3 Virtualization Server Set Configuration

The Virtualization Server Set device manages the top-level server set configuration properties and the hierarchy of Virtualization servers and VMs owned by the server set. The following figure illustrates the Control Server Set device editor in ToolboxST, with the configuration properties displayed in the Property Editor (lower left) and the topology editor (right side).
### 9.3.1 Virtualization Server Set Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Revision</strong></td>
<td></td>
</tr>
<tr>
<td>Major Revision</td>
<td>Time of the last component build that occurred after a major change had been made to the component. When a major change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td>Minor Revision</td>
<td>Time of the last component build that occurred after a minor change had been made to the component. When a minor change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Free form text field used to provide a user friendly description of the VM to operators and maintenance personnel. The Description is displayed by the Control System Health Viewer.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Set to True if the server set has multiple Virtualization Servers configured for High Availability.</td>
</tr>
<tr>
<td>Producer ID</td>
<td>Unique identifier for the server set. This value is automatically generated and typically should not be modified by the user.</td>
</tr>
<tr>
<td><strong>Hypervisor</strong></td>
<td></td>
</tr>
<tr>
<td>Hypervisor Type</td>
<td>Type of hypervisor hosted by the servers in the server set. Control Server setting is ESXi.</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the read-only hypervisor account used by the CSH feature for collecting status data.</td>
</tr>
<tr>
<td>Password</td>
<td>Password configured for the read-only hypervisor account used by the CSH feature for collecting status data from the servers.</td>
</tr>
<tr>
<td><strong>vSphere</strong></td>
<td></td>
</tr>
<tr>
<td>vCenter Host</td>
<td>Host name or IP Address of the vCenter Server VM (typically named HC1) that is managing the server set.</td>
</tr>
<tr>
<td>vCenter Username</td>
<td>Username of the read-only vSphere account used by the CSH feature for collecting status data from vCenter.</td>
</tr>
<tr>
<td>vCenter Password</td>
<td>Password configured for the read-only vSphere account used by the CSH feature for collecting status data from vCenter.</td>
</tr>
</tbody>
</table>
9.3.2 Manage Virtual Devices

The right side of the Virtualization Server Set device window is used to manage the association of the virtual devices to the server set. Servers are added directly to the server set in a Simplex server set, and are added to the Cluster in an HA server set. VMs that run on a single server are added directly to the server, while VMs in an HA server set can also be added to the Cluster to specify VMs that migrate between servers using the HA feature. A virtual device is added by right-clicking on the Server Set, Cluster, or Server that owns the component and selecting “Add”.

➢➢ To add a virtual device

1. Right-click the Server Set, Cluster, or Server that owns the component and select Add.

![Enter a Device Name and Device Type](image)

2. Enter the device name, select the device type from the drop-down menu, and select OK to create the virtual component association.

➢➢ To remove a virtual device: right-click the device and select Delete.
9.4 Virtualization Server Configuration

The Virtualization server reflects both the physical server hardware and the hypervisor running on each server.
### 9.4.1 Virtualization Server Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Revision</strong></td>
<td></td>
</tr>
<tr>
<td>Major Revision</td>
<td>Time of the last component build that occurred after a major change had been made to the component. When a major change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td>Minor Revision</td>
<td>Time of the last component build that occurred after a minor change had been made to the component. When a minor change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Cluster Name</td>
<td>Name of the High Availability Cluster of which the Virtualization Server is a member. VMs in the cluster can migrate between servers that are cluster members. This value is blank if the server is part of an HA enabled server set but is not a member of the cluster. This value is also blank for Simplex server sets, since a Simplex server set has only one server and therefore does not provide an HA cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Free form text field used to provide a user friendly description of the Virtualization Server to operators and maintenance personnel. The Description is displayed by the CSH Viewer.</td>
</tr>
<tr>
<td>Management Network</td>
<td>Name of the network used to gather data from the Virtualization Servers and vCenter in the case of an HA server set.</td>
</tr>
<tr>
<td><strong>Hypervisor</strong></td>
<td></td>
</tr>
<tr>
<td>Hypervisor Agent Account Override</td>
<td>Default value of False instructs the CSH feature to use the Hypervisor username and password settings defined at the Virtualization Server Set level. In most cases, all of the servers in the server set will use the same username and password; however, it is possible to configure unique usernames and passwords for each server. In the case of unique server passwords, the Hypervisor Agent Account Override can be set to True and the unique username and password can be defined for each server.</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the read-only hypervisor account used by the CSH feature for collecting status data.</td>
</tr>
<tr>
<td>Password</td>
<td>Password configured for the read-only hypervisor account used by the CSH feature for collecting status data from the servers.</td>
</tr>
</tbody>
</table>
9.4.2 Configure Network Settings

➢ To configure network settings: create a network connection for each server device in ToolboxST for the PDH/Management network.

➢ To configure network settings using vSphere Client: open the HS1 server device in ToolboxST and enter the network name and IP address for the Network Adapter.
To determine network settings using vSphere Web Client

1. Open a web browser and connect to vCenter. Refer to Appendix B Connect to vCenter with Web Client.
2. Select the server from the Tree View, then select the Manage tab and select Networking.

This figure shows the vSphere Web client connected to the HS1 server. Select each virtual switch until the Management Network is found. The PDH network shares the management network interfaces with the Management Network, and the management IP address is 172.16.199.8.
3. Open the HS1 server device in ToolboxST and enter the network name and IP address under the Network Adapter.
9.4.3 Configure Management Network Switch Connections

➢➢ To configure management network switch connections

1. Open the Network Switch device in ToolboxST and select the port where the primary server management network interface is connected.

2. Select the primary PDH (Management) connection for the server as shown in the following figure.

   Note The Port Connection type must be Default_NativeDeviceConnectionOrNotUsed.

3. Click OK to add the connection. The Network and IP Address fields will be automatically populated.

4. (Optional) Enter a description in the Port Description field.

5. Repeat this process for the backup management network connection. The following figure shows the primary and backup management connections for all of the servers in an HA server set.
Note Primary and backup connections are not made to the same switch in real-world systems, but both are shown on the same switch in this example to illustrate the concept.

9.4.4 Configure Non-Management Network Switch Connections

➢➢➢ To configure non-management network switch connections

1. Add the server network connections to the switch for the remaining server network interfaces.

2. Open the Network Switch device in ToolboxST, select the port, and change the Port Connection type to Server.

3. Add a description in the Port Description field (for example HS1 UDH Primary) to identify the server, network, and redundancy of the connected network. The following figure shows all of the management and UDH network connections for an HA server set.
9.5 Virtual Machine Configuration

The VM configuration in ToolboxST consists of the configurable properties listed in the following section.

![Configuration Revision and General properties](image)

### 9.5.1 VM Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Revision</strong></td>
<td></td>
</tr>
<tr>
<td>Major Revision</td>
<td>Time of the last component build that occurred after a major change had been made to the component. When a major change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td>Minor Revision</td>
<td>Time of the last component build that occurred after a minor change had been made to the component. When a minor change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Critical</td>
<td>Used to specify if the VM is considered critical to the system. The default value is True. The CSH feature will generate alarms if a VM marked as Critical is not running or is reported by the hypervisor to be in an abnormal state.</td>
</tr>
<tr>
<td>Description</td>
<td>Free form text field used to provide a user friendly description of the VM to operators and maintenance personnel. The Description is displayed by the CSH Viewer. The following descriptions are a good start for the infrastructure VMs. CA1: Certificate Authority Server DC1: Primary Domain Controller DC2: Backup Domain Controller HC1: VMware vCenter Appliance HW1: VMware Witness Appliance</td>
</tr>
</tbody>
</table>
9.5.2 Configure Network Settings

➢ To configure network settings

1. Add a network adapter for each network to which the VM is connected.
2. Enter the IP address and select the connected network from the Network drop-down menu.

VM network connections can be discovered for both HA and Simplex server sets using the vSphere Client.

3. Select the VM, then navigate to the Manage\Settings tab. The Network Adapters are displayed beneath the VM Hardware selection.
The VM Network connections can also be discovered using the vSphere Web Client for HA systems.
9.6 Thin Client Configuration

➢ To configure the Thin Client

1. From the ToolboxST System Editor Tree View, right-click the system item and select Insert New, Control Server, and Thin Client.

2. Open the Thin Client component to display the configuration properties in the Property Editor.
### 9.6.1 Thin Client Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Revision</td>
<td>Time of the last component build that occurred after a major change had been made to the component. When a major change is made, the revision is set to zero until a build occurs.</td>
</tr>
<tr>
<td>Major Revision</td>
<td>Time of the last component build that occurred after a minor change had been made to the component. When a minor change is made, the revision is set to zero until a build occurs.</td>
</tr>
</tbody>
</table>

**General**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Free form text field used to provide a user friendly description of the VM to operators and maintenance personnel. The Description is displayed by the CSH Viewer.</td>
</tr>
<tr>
<td>DHCP Enabled</td>
<td>Set to True if Domain Services are enabled in the system. If True, the Thin Client will be monitored using the host name specified in the Network Settings or using a default host name manufactured from the MAC address if a host name is not provided.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Uniquely identifies the Thin Client. The MAC address is provided on the pull out tab on the Thin Client.</td>
</tr>
<tr>
<td>Manufacturer Type</td>
<td>Specifies the manufacturer of the Thin Client terminal</td>
</tr>
<tr>
<td>Model Number</td>
<td>Model number of the Thin Client. The model number is provided on the pull out tab on the Thin Client.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Thin Client</td>
</tr>
<tr>
<td>Operating System</td>
<td>Operating system running on the Thin Client.</td>
</tr>
</tbody>
</table>

### 9.6.2 Configure Network Settings

The CSH feature uses the MAC Address and DHCP Enabled settings and the Network Adapter settings to determine how to monitor the Thin Client terminal status. When DHCP is disabled, the CSH feature uses the specified IP address to monitor the Thin Client status. When DHCP is enabled, the CSH feature uses either the specified Host Name or, if a Host Name is not specified, it attempts to use a manufactured host name based on the Thin Client terminal’s MAC address. The default host name follows the Dell™ Wyse™ terminal standard so the host name must be entered for Thin Client terminals from other manufacturers, such as HP®. The Host Name must also be specified in cases where a Dell Wyse Thin Client terminal’s host name has been modified from its default value.

**Note** The CSH feature in WorkstationST releases prior to V07.04.02C (included in ControlST versions prior to V07.04.00C SP01) did not use the Host Name value. Dell Wyse Thin Client terminals must retain their default host name values, and Thin Client terminals from other manufacturers, such as HP, must be configured with a Dell default formatted host name based on the operating system of the Thin Client terminal as follows:

- Windows 7 WES<MAC address> example: WES008064F6101D
- Windows 10 WIE<MAC address> example: WIE008064F6101D
- SUSE® Linux™ LWT<MAC address> example: LWT008064F6101D
➢ To disable the DHCP Enabled network adapter setting

1. Open the Thin Client component to display the configuration properties in the Property Editor.

2. From the Tree View, select the Network Adapter # item to display the network to which the Thin Client is connected and modify the Network Adapter settings.

3. Leave the Host Name property blank or specify a Host Name (optional since it is not used in this case).

4. Enter the unique IP Address of the Thin Client.

➢ To enable the DHCP Enabled network adapter setting

1. Open the Thin Client component to display the configuration properties in the Property Editor.

2. From the Tree View, select the Network Adapter # item to display the network to which the Thin Client is connected and modify the Network Adapter settings.

3. Modify the Host Name property as follows:
   a. If the Thin Client terminal is a Dell Wyse model with the default host name configured by the manufacturer, leave the Host Name blank.
   b. If the Thin Client terminal is not a Dell Wyse model, or it is a Dell Wyse model with a modified host name, provide the Host Name value that matches the host name of the Thin Client terminal.

4. Enter a unique IP Address that does not conflict with any other devices on the configured network. This value is not used by the CSH feature, but a value must be entered to prevent ToolboxST build errors.
9.6.3 Configure Network Switch Connections

➢ To configure network switch connections
1. Open the Network Switch device in ToolboxST and select the port to which the Thin Client is connected.

*Note* The Port Connection type must be Default_NativeDeviceConnectionOrNotUsed.

2. Select **OK** to add the connection. The Network and IP Address fields are automatically populated.
3. (Optional) Enter a description in the Port Description field.

*Example Configured Port Connection*
10  **OPC® UA Communication**

The CSH viewer uses an OPC UA client to connect to the WorkstationST OPC UA on the CSH configured node.

10.1  **Client/Server Connection Sequence**

When an OPC UA client and server connect, both the client and the server application have an X509 certificate they own. For successful communication, both the OPC UA client and server must receive each other’s certificate over the communication link and verify that it matches a certificate in the trusted store location. The OPC UA client and server use the Windows local machine certificate store as the trusted store, which is located within the folder *UA Applications* on the computer where they are running.

![Diagram of Client/Server Connection Sequence](image)

**Note**  Refer to the *WorkstationST OPC UA Server Instruction Guide* (GEI-100828), the section *Application Certificates* for further details.
## 10.2 Application Certificate Sharing

To share the application certificates between the CSH viewer (viewer) and the WorkstationST OPC UA Server (server), both certificates must reside in the Windows local store (trusted store for both client and server) on both the viewer computer and the server computer. (If both the viewer and the server are running on the same computer, they will already be in the same trusted store and no further action is required for the local viewer to communicate with the server).

➢ To share the certificates

1. Open the **CSH viewer** at least one time. The first part of the connection conversation will cause the client (viewer) to talk to the server. The server sends back its application certificate and the client looks in the trusted store to see if the server is trusted. Initially, the server’s certificate will be missing from the client’s trusted store. Use the Certificate Manager to trust the server’s certificate on the client node:
   
   a. Select the **WorkstationST Status Monitor** tray icon to display **WorkstationST Status Monitor**.
   
   b. From the **Tools** menu, select **Certificate Manager** to display the WorkstationST Certificate Manager.

   ![Certificate Manager](image)

   c. Click the **Rejected** toolbar icon to display a list of all rejected certificates.

   d. From the **CSH** node, select the WorkstationST OPC UA server certificate and click **Trust Selected Certificates** to trust it.

2. Open the **CSH viewer** again. This time the client (viewer), will trust the server and will send the certificate to the server. Use the certificate manager to trust the server’s certificate on the CSH server node:

   a. From the **Tools** menu, select **Certificate Manager** to display the WorkstationST Certificate Manager.

   b. Click the **Rejected** toolbar icon to view the client’s certificate and click **Trust Selected Certificates** to trust it.
At this point, when the viewer is started it should be able to talk to the server.

11 Control System Health Viewer

The CSH Viewer displays information obtained by the CSH server. The server contains health and status information for controllers, networks, NTP, workstation computers, and the WorkstationST application. The viewer is a stand-alone product that is run from the Start menu > All Programs option.

The viewer will attempt to connect to the CSH server when started. If the location of the server is unavailable to the viewer, or the user wishes to connect to a different server, the ability to enter the Host Name or IP address of the CSH server is available from the View menu. Access to the CSH server is dependent on the viewer and server having the appropriate application certificates.
The CSH Viewer displays the data collected by the CSH management system. The data is grouped to understand system status and make problems easier to diagnose as follows:

Select an item in the **Tree View** and select the **Status** tab to display the health status of the item.

The bottom pane displays information messages and/or log messages.

Click the **Refresh** button to update the information on the **Diagnostics** tab.

The **Control System Health Viewer** provides only high level network and device status information. Further details about the network switches, their detailed port status information, and details about the connected devices can be obtained by starting the **Network Status Viewer** using the icon provided in the **Control System Health Viewer** menu bar.

**CSH Viewer Help** is available from the **Help** menu item.
Control System Health Viewer displays the Control System Health Instruction Guide (GEI-100834).

Certificate Management displays instructions on managing the security certificates required for the viewer and server.

About displays the information on the current version of the viewer.

11.1 Virtualization Platform Health Information

The Virtualization Platform node of the Control System Health Viewer displays the health information for Control Server. The Control System Health Viewer provides a hierarchical view of the servers that make up a Control Server Set and the VMs hosted by them.

➢➢ To view virtualization platform health information

1. From the Tree View, expand the Virtualization Platform node to display the server sets.

2. Expand each server set to display the servers within it.
3. Expand the VM’s nodes to display the VMs hosted by each server and server set.

4. Select a component to display component status information in the right status pane.
11.1.1 Server Status Information

➢ To view server status information: expand a Server node to display additional status nodes.

➢ To view CPU information: expand the CPU node to display critical capacity and usage information.
➢ **To view Datastore information:** expand the **Datastore** node to display critical Capacity and Usage information for each server Datastore, including the status reported by VMware.

➢ **To view hardware health information:** expand the **HardwareHealth** node to display status information for the critical server hardware subsystems reported by the hypervisor.

Each Hardware Health sub node provides status information for hardware subsystem.
Once hardware issues are identified, the vSphere Client is used to locate the offending hardware component(s).

Refer to Appendix C Identifying Server Hardware Issues for further details on identifying specific hardware issues.
➢ To view server hardware information: expand the **HardwareInfo** node to display server hardware details including:

- Model and Service Tag
- Bios Version
- CPU and Memory Capacity

➢ To view Hypervisor information: expand the **HypervisorInfo** node.
➢ To view **Memory information**: expand the **Memory** node to display critical server memory capacity and usage information.

![Memory node example](image)

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server memory capacity in Gigabytes</td>
<td>63</td>
</tr>
<tr>
<td>Server Memory Status</td>
<td>OK</td>
</tr>
<tr>
<td>Server memory usage has exceeded the alarm</td>
<td>False</td>
</tr>
<tr>
<td>Server memory usage in Megabytes</td>
<td>0</td>
</tr>
<tr>
<td>Server percent free memory</td>
<td>48</td>
</tr>
</tbody>
</table>

➢ To view **Network information**: expand the **Network** node to display status information for each Network to which the server is connected.

![Network node example](image)

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The network connection status</td>
<td>OK</td>
</tr>
<tr>
<td>The network name</td>
<td>PDH, Management Network</td>
</tr>
<tr>
<td>The Virtual Switch hosting this network</td>
<td>vSwitch0</td>
</tr>
<tr>
<td>Total Number of Adapters for this network</td>
<td>2</td>
</tr>
</tbody>
</table>
The Network Adapter nodes provides:

- Status information for each adapter
- Visual indication of network connection redundancy

➢➢➢

To view VSAN Health information: expand the VsanDisk node to display critical Health information for each server VSAN disk.
11.1.2 Virtual Machine Status Information

The VM nodes provide the following information:

- Server the VM is currently running on
- Status as reported by VMware
- Power state of the VM
- VM description as configured in ToolboxST

➢➢ To display additional VM status nodes: expand the VM node.

➢➢ To view CPU information: expand the CPU node to display critical capacity and usage information.
➢ To view guest operating system information: expand the **GuestInfo** node to display information about the type and state of the VM operating system.

➢ To view memory information: expand the **Memory** node to display critical memory capacity and usage information.

➢ To view storage information: expand the **Storage** node to display information about the capacity and usage of the server storage allocated to the VM.
➢ To view virtual desk information: expand the `VirtualDisk_#` nodes to display information about the capacity and usage for each of the Virtual Disks within the VM.

11.2 WorkstationST Computer Health Information

Computer Health displays the health status for all workstation computers in the system.

➢ To display WorkstationST Computer Health information

1. From the Tree View, select the WorkstationST Computer Health item to display all computer diagnostic alarms related to the system workstations on the Diagnostics tab.
2. Expand the WorkstationST Computer Health item to display the system workstation computers and their health in the Tree View.
3. Select a workstation item (Wkstn 1 for this example) to display additional hardware status, including fan status and memory usage, on the Status tab.
4. Expand the workstation item (Wkstn 1 for this example) to display the overall health for the computer’s disk drives, network adapters, and processors in the Tree View.
5. Expand the Disk, Network, and Processors items to display the status of each disk drive, network adapter, and processor in the Status tab.
6. Select an item (Disk_1 for this example) to display the diagnostic alarms associated with that item in the Diagnostics tab.
11.3 Controllers Health Information

The Controllers information provides the health status for all units in the system.

**Note**  CSH does not monitor PFFA I/O (FOUNDATION Fieldbus™) at this time.

➢➢ To display Controller health information

1. Select the Controllers item to display the overall health of all of the system controllers and I/O packs in the Status tab.
2. Expand the Controllers item to display the overall health of all of the system units (G1 for this example) in the Tree View.
3. Select a unit (A6e for this example) to display the diagnostic alarms associated with all of the unit controllers and I/O packs in the Diagnostics tab.
4. Expand a unit (A6e for this example) to display the health information for all of the controllers in the unit. Simplex controllers will have a single controller and TMR controllers will have three. The expanded unit view also includes the overall health of the I/O modules associated with the unit.
5. Select a controller (A6e-R for this example) to display the details of that controller on the Status tab. The Diagnostics tab will display only the diagnostic alarms associated with the selected controller.
6. Expand the IoModules item to display all of the I/O modules in the unit. They can be Simplex or TMR. Select the Diagnostics tab to display all I/O pack diagnostic alarms for all I/O modules.
7. Select an I/O module (PHRA-21 for this example) to display diagnostic alarms for the I/O packs in the module in the Diagnostics tab.
8. Expand an I/O module (PHRA-21 for this example) to display the status of all of the module I/O packs in the Tree View.
9. Select an I/O pack (PHRA-21-R for this example) to display the details of its health on the Status tab.
10. Select the Diagnostics tab to display the diagnostic alarms associated with the selected I/O pack.
11.4 **Networks Health Information**

The Networks information displays the overall health of the control system networks.

➢ **To display Networks health information**

1. Select the **Networks** item to display the overall status for all of the control system networks in the **Status** tab.

2. Expand the **Networks** item to display the overall health of the **Devices**, **Networks**, and **Switches** in the **Tree View**.

3. Expand the next level **Networks** item and select a network (**PDH** for this example) to display health details on the **Status** tab.

4. Select the **Switches** item to display the overall status for all of the network switches that make up the control system networks in the **Tree View**.

5. Expand the **Switches** item and select a switch (**Cisco3750** for this example) to display the switch details in the **Status** tab.

6. Expand the **Devices** item to display the overall health of all of the controllers and workstation computers in the **Tree View**.

7. Select a device (**wkstn 1** for this example) to display the status of all of its network connections in the **Tree View**. Select the **Diagnostics** tab to display associated network alarms.

8. Expand a device (**wkstn 1** for this example) and select a network connection (**LegacyUdh** for this example) to display the status details of the network connection.

---

**Note** Further details about the status of the device’s actual and configured network switch connections can be obtained by starting the Network Status Viewer.
11.5 **Network Time Protocol Health Information (Time Synchronization)**

Time-stamped data is critical to monitoring and troubleshooting the control system. The control system uses NTP running on the workstation computers and controllers to maintain time within a few milliseconds between all of the computers and controllers in the system.

➢ To display NTP health information

1. Select the **Ntp** item to display the overall status of the time synchronization in the **Status** tab.
2. Expand the **Ntp** item and select a device (**A6e-R** for this example) to display detailed NTP status information for that device in the **Status** tab. Select the **Diagnostics** tab to display the NTP related diagnostic alarms for the selected device.
11.6 **WorkstationST Feature Health Information**

The WorkstationST Feature Health information monitors the health of all the workstations and the WorkstationST features in the control system.

➢ To display WorkstationST Feature Health information

1. Select the **WorkstationST Feature Health** item to display the overall status for all of the WorkstationST features running on all of the workstation computers in the system in the **Status** tab.

2. Expand the **WorkstationST Feature Health** item to display all of the workstation computers in the system.

3. Expand a workstation item (**wkstn1** for this example) to display the status of WorkstationST features running on that computer.

4. Select a feature (**Alarm Server** for this example) to display the status details of that feature in the **Status** tab.
12 Network Status Viewer

The Network Status Viewer gives the detailed view of the configured device connections, the actual connections, and the status of the network switch ports. The Network Status Viewer can be started as a standalone tool from the system start menu and it can also be started directly from the Control System Health Viewer.

➢ To start the Network Status Viewer: from the Start menu select All Programs, GE ControlST, WorkstationST, and Network Status Viewer.

Or

From the Control System Health Viewer toolbar, click the Network Status Viewer icon.
12.1 **Network View Tab**

The Network View tab displays the network hierarchy; the networks are the top-level items. The switches are at the next level, followed by the devices.
12.2 Device View as Configured Tab

The Device View As Configured tab displays the devices in their configured locations, as well as deviations of the device connections from their configured locations. This is used to find occurrences of a device connected to the wrong port that is masking the location of an offline device configured to be connected to that port.
The following figure displays the configured and connected device views with the switch connections expanded.
12.3 Device View by Connection Tab

The Device View By Connection tab displays the actual location of each device by the network switch and port.
12.4 Network Troubleshooting Example

The following is an example of the Network Status Viewer being used to determine any network issues, the devices affected, and the cause.

The sample screen displays no issues with the LegacyUDH, one error on the UDH, and a topology error on the PDH networks.
Expand the **UDH** item to display the network issues.

Expand **Switch2** to display all issues related to the switch.

This example shows that multiple devices configured to be connected to this switch are offline, and several others are online but not connected in their configured locations.
13 Control System Health Feature Alarms

Controllers and I/O packs generate diagnostic alarms when an abnormal condition is detected. These alarms are collected by the system Alarm Server and displayed in the Alarm Viewer. The CSH management system independently scans the controllers, I/O packs, switches, computers, and such, and generates alarms when abnormal conditions are detected. The Alarm Server connects to the CSH server to receive these alarms.

The Alarm Server connection to the CSH server is configured on the WorkstationST Alarms tab by entering the Hostname or IP address of the workstation running CSH as shown in the following figure.

Note CSH is not critical to the operation of the plant and has not been designed to support multiple instances in a single system. One workstation in the system will run CSH and all Alarm Servers will connect to it in order to get a consistent view of alarms between both standalone and redundant Alarm Servers.
The following figure shows alarms generated by the CSH management system.

Note In the previous figure the alarms generated by the CSH management system includes multiple alarm classes. The CSH management system categorizes the alarms by subsystem using the alarm class in order to facilitate troubleshooting subsystem issues. For example, all NTP subsystem related alarms can be displayed by filtering on only alarms with the NTP alarm class.

The following table lists the subsystems monitored by the CSH management system and their corresponding alarm classes.

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Alarm Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Health</td>
<td>Netwk</td>
</tr>
<tr>
<td>Controller and I/O Pack Health</td>
<td>ControllerHealth</td>
</tr>
<tr>
<td>Workstation Computer Health</td>
<td>PcHealth</td>
</tr>
<tr>
<td>Time Synchronization System Health</td>
<td>NTP</td>
</tr>
<tr>
<td>WorkstationST</td>
<td>None</td>
</tr>
</tbody>
</table>
14 Troubleshoot Network Switch SNMP Issues

The most common issue associated with the CSH is the inability to get SNMP data from one or more network switches. This results in topology errors due to the CSH’s inability to determine which ports the devices are connected to, as well as a lack of port level data. Failure to read SNMP data from a network switch is typically the result of SNMP settings in ToolboxST that do not match the network switch SNMP configuration. For the SNMP V1 protocol, this results from an incorrect SNMP V1 Community setting. For the SNMP V3 protocol, this may be the result of an incorrect setting for the SNMP V3 User Name, and/or invalid SNMP V3 Authentication and Encryption passwords. Telnet into the switch to determine the SNMP settings and verify that the SNMP settings in ToolboxST are correct.

**Note** SNMP is a simple network management protocol for managing devices on internet protocol networks.

The recommended way to determine if CSH is receiving SNMP data from the switch is to hover over the switch in the Network Status Viewer to display the system information (System Info), which provides the SNMP value read from the switch. If System Info is blank, CSH is not able to read SNMP data from the switch.

Another method to determine if the CSH is receiving SNMP data from the switch is to expand one or more ports to see if the data has been updated. If the values are all zero and port description (first field) is blank, SNMP data has not been read for that port. This would normally coincide with failure to read SNMP data for the entire switch.
The following figure shows the expected Network Status Viewer display, including a legitimate topology error:
Note Some Allied Telesis switch models do not accept special characters such as the @ symbol, so these switches cannot use the standard GeS@lem9ro SNMP community name. This is a common configuration error where all of the switches are configured with the default community name, while certain switches are using a different community name.
Notes
Appendix A Connect to Server with vSphere Client

The vSphere Client application is used to connect to an ESXi server and get status and configuration information.

➢ To connect to a server with vSphere Client

1. Launch the vSphere Client from a computer or VM with the vSphere Client application installed.
2. Login to the vSphere client. Enter the IP address of the server and the User name and Password for the CSH user account on the server.

The vSphere Client window is displayed.
vSphere Client Window
Appendix B Connect to vCenter Web Client

Use a web browser to connect to the vCenter Appliance VM in a High Availability (HA) Server Set to get configuration and status information for all servers and VMs in the Server Set.

➢ To connect to the vCenter Web Client

1. Open a web browser and open the vCenter URL (typically 172.16.199.7).
2. From the VMware vSphere welcome window, select Log in to vSphere Web Client.

3. Enter the vCenter User name and Password, then click Login.
The vSphere Web Client is displayed.
Appendix C Identifying Server Hardware Issues

The Hardware Health node beneath each server in the Control System HealthViewer provides a summary of the hardware status items reported by the ESXi hypervisor.

The following figure shows that there are 13 Fan status items with a normal status, and no items with an Alert or Warning status. Further information can be obtained using the vSphere Client or the vCenter Web Client for a server in a HA Server Set.
The following figure shows the hardware status information in the vSphere Client.

Expand the Fan status to display the status of the 13 individual Fan status items.
The following figure shows hardware status from the vSphere Web Client view.
Example: Redundant Power Supply Failure

The following example illustrates the process for identifying hardware failure. For this example, the power was unplugged from the redundant server power supply. The following figure shows that the HardwareHealth node is indicating a failure, and the Power node is showing an error condition.

Selecting the Power node displays one Power item with an Alert state and one Power item with a Warning state in the Status tab view.

The Diagnostics tab also indicates this condition. The alarm text indicates that there is at least one item in the Power category indicating an Alert condition.
For more information about this failure, launch the vSphere Client application, connect to the HS1 Server, and select **Health Status** within the Configuration tab.

The Power node indicates an Alert status. Expand the Power node to display the status of all the Power items. The item with the Alert indicates the cause of the failure in this case: **Power Supply 2 Status 0: Power Supply AC Lost**. Restore the power connection to the redundant power supply to clear this condition.
Appendix D Resolve Failure to Get vSphere Data Issues

If CSH is unable to log in to the ESXi hypervisor on the server it will not be unable to read the vSphere data. The data will be displayed as Unhealthy in the Control System Health Viewer, and an alarm indicating the login failure is generated.

CSH reports the following alarm when it cannot log in to vSphere to get data:
Unable to get vSphere data from Server <<server>> due to a login failure. Verify that the Hypervisor Username and Password are correct.

Verify that the hypervisor user name and password specified in the Control Server Set device in ToolboxST matches the actual hypervisor username and password.
Hypervisor Login Credentials in ToolboxST
Appendix E Troubleshooting vCenter Alarm Monitoring Issues

CSH reports the following alarm when it cannot log in to vCenter to retrieve alarm data:
Unable to monitor alarms for vCenter on host <ipAddress> due to a login failure

Verify that the vSphere username and password specified in the Control Server Set device in ToolboxST matches the actual vSphere username and password.
Appendix F Trending Control System Health Data Example

All of the data that the CSH feature collects is published to the system OPC UA server and can be viewed using Trender for the HMI application. The following example illustrates the procedure for trending CSH data.

➢ To create a trend to view CSH data

1. Open the Trender for the HMI application.
2. Select Edit/Add Traces… from the main menu to open the Trender Add Trace Wizard.
3. Select Live for the trend type.

4. Select OPC-UA Server as the data source.
5. Enter the OPC-UA server information.

6. Enter the trend period in mS.
7. Click **Add** to display the *Select a Variable* dialog box.

All Control System Health variables are located beneath the CSH node.

8. Expand the CSH node and navigate to the appropriate data item for trending.
9. Click **Finish** to add the variable to the trend.
10. Click **Record** in the lower left corner to begin trending the data.