
Introduction

This System Release Note (SRN) provides information about the GridTime™ 3000 GNSS Time Server version **v1.2r0.0** to be released in June 2026. Release version **v1.2r0.0** is the firmware release notes for the GridTime 3000 and covers all resolved and known issues.

Table of Contents

Introduction.....	1
1. Summary of Features.....	3
1.1. New Features in v1.2r0.0.....	3
1.2. Known Issues.....	3
1.3. Resolved Issues.....	9
2. Upgrading the Firmware.....	15
2.1. Upgrading the Firmware.....	15
3. Contacting Technical Support.....	19
4. References.....	20
5. Revision History.....	21
Microchip Information.....	23
Trademarks.....	23
Legal Notice.....	23
Microchip Devices Code Protection Feature.....	23

1. Summary of Features

This section describes the new features, known and resolved issues included in this software release notice.

1.1. New Features in v1.2r0.0

- Synchronous Ethernet (SyncE) Input and Output functions
- Added customizable login banner
- Added Password Configuration Options
 - Customizable minimum and maximum password length
 - Configuration to enforce usage of uppercase, lowercase, numbers or symbols in a password
 - Configuration to check password against a list of common exploited passwords
 - Configuration to check password does not include the user's username
 - Configuration to enforce a password expiration
- Added an idle timeout feature with configurable idle duration
- Added an inventory page that includes:
 - Part number
 - Serial number
 - Power supply variants fitted
 - Oscillator Fitted
 - Licenses installed
 - MAC address of each Ethernet port
 - Firmware version
- Ability to set SNMPv3 privacy/encryption and authentication keys independently
- Added AES128 and AES256 cryptography to SNMPv3 privacy/encryption key
- Added SHA1 and SHA256 cryptography to SNMPv3 authentication key
- Added LCD alarm, syslog notification and SNMP trap for if the log file fails to capture information
- Updated operating system to Yocto 5.0.14 (Scarthgap)
- Updated `Node.js` to 20.19.2
- Updated `NestJS` to 11.1.19
- Updated `Angular.js` to 21.1.5

1.2. Known Issues

The following tables list the known issues in v1.2r0.0, their operating constraints and workarounds.

1.2.1. Additional Device Functions

The following table lists the known issues with the general function of the device, including any issues related to output suppression, daylight savings rollover, licenses or expansion oscillator usage.

Table 1-1. Known Issues: General Functions of the Device

Issue Reference	Known Issue	Workaround
GT3K-10279	When GNSS is disabled, the priority 1 source is no longer displayed.	Recommended to use priority 2 as the highest level.

Table 1-1. Known Issues: General Functions of the Device (continued)

Issue Reference	Known Issue	Workaround
GT3K-10307	GridTime™ 3000 GNSS Time Server exits Holdover 6 - 7 seconds earlier than the specified configuration when Holdover Time is enabled.	—

1.2.2. Clock Management Tool (CMT)

The following table lists the known issues with the CMT, including any field validation errors and issues with any buttons or configurable options.

Table 1-2. Known Issues: CMT Related Functions

Issue Reference	Known Issue	Workaround
GT3K-4438	It is possible to click save on the PRP Port B – saving over the duplicated configuration from Port A.	—
GT3K-5436	When enabling or disabling some settings in the CMT, the browser must be refreshed after saving to reflect the changed settings.	—
GT3K-10277		—
GT3K-10245	When the GridTime™ 3000 GNSS Time Server sees the PTP Announce messages from two PTP timeTransmitter, the GM ID displayed on the Dashboard's Available sources will toggle between the two GM IDs.	—
GT3K-10254	After a user has configured source priority 1, 2, 3 or 4, saved and then navigated to another page, when returning to priorities, these display the default values instead of the configured values.	The back end systems continue to change the source, and this issue is graphical only.
GT3K-10264	When the Test mode is configured to a time earlier than 01/01/1970 00:00:00 UTC, the time on the dashboard does not reflect the time configured.	—
GT3K-10276	The Link Active indicator continues to show even if only one port of a PRP pair is connected.	Noting that PRP alarms still continues to operate.
GT3K-10290	On the CMT dashboard, an IRIG-B input reports the index of the port instead of the port number as defined on the product decal.	—
GT3K-10299	The “TEST” source can sometime appear on the dashboard's list of available sources even when not used.	—
GT3K-10346	Dashboard reports previous virtual port PTP PortState for LANB.	—
GT3K-10376	CMT allows invalid loopback IP address (127.0.0.0) for NTP Server configuration.	—
GT3K-10386	“DHCP Request Interval” accepts invalid values (characters) in Firefox browser.	—
GT3K-10387	Dashboard Location co-ordinates report all zeroes when powered on with GNSS disabled then brought into GNSS Sync.	—
GT3K-10391	Shows inconsistent session timeout behavior and logging.	—

1.2.3. Authentication

The following table lists the known issues with the authentication of users through a local or an external authentication provider and any issues with access control.

Table 1-3. Known Issues: Authentication

Issue Reference	Known Issue	Workaround
GT3K-3444	Each time an LDAP login attempt is made, the GridTime™ 3000 GNSS Time Server establishes a new connection to the configured LDAP server, but it does not close any previously made connections. The previous connections are left idle indefinitely.	To close idle connections, configure the LDAP server.
GT3K-3461	When a RADIUS login is attempted and the RADIUS server does not respond, a “Maximum retries exceeded” error message appears, instead of a “Server not found” message.	—
GT3K-3464	If the RADIUS “Server: Retries” setting is configured to be 0, the number of retries performed is 3.	—
GT3K-3527	When two users have the same username, both are deleted when the delete button is selected.	Ensure that each user has a unique username.
GT3K-5634	The GridTime 3000 GNSS Time Server ignores access reject response from a RADIUS server and continues to send retry access requests.	—
GT3K-5755	When a LDAP server is unreachable, no timeout or “Login Failed” message is displayed.	—
GT3K-10249	LDAP failed login attempts are not logged out with the required LDAP-specific details.	—
GT3K-10288	GridTime 3000 GNSS Time Server allows any file type to be uploaded into the CSR upload function.	This is only on the initial upload; rgw CSR is validated when being applied to the device and does not allow file types other than .key or .cert to be applied.
GT3K-10377	Unable to save changes to device login provider.	—
GT3K-10378	CMT access is denied when RADIUS user is authenticated successfully by the RADIUS Server.	—

1.2.4. Simple Network Management Protocol (SNMP)

The following table lists the known issues with SNMP including any issues with SNMP authentication, SNMP traps, or SNMP configuration.

Table 1-4. Known Issues: SNMP

Issue Reference	Known Issue	Workaround
GT3K-5295	IRIG-B input notifications will not be sent on start up when there is an input enabled.	—
GT3K-10289	The CMT forces a privacy password to be set even when privacy is set to none.	—
GT3K-10343	Clock state reporting of SNMP notifications on management over Timing Port is incorrect.	—

1.2.5. IPv4 Ethernet

The following table lists the known issues with the network ports including both the administrator and timing ports, their interfacing protocols and logging.

Table 1-5. Known Issues: Networking Related Issues

Issue Reference	Known Issue	Workaround
GT3K-2743	When a device on the network is present with the GridTime™ 3000 GNSS Time Server's preferred link local address, and when no DHCP server is present on the network, the GridTime 3000 GNSS Time Server first sends a DHCP Decline message and then restarts the DHCP discovery again, before falling back to an alternative link local IP address.	—
GT3K-3036	Issue with admin Ethernet port behavior: Unexpected Source IP address in DHCP request message after link local fallback.	—
GT3K-5737	When set to link local IP address mode, no probe packets are observed.	—
GT3K-10265	Copper Ethernet ports ETH1 and ETH2 do not emit or respond to network traffic when operating in half-duplex mode.	—
GT3K-10296	When DHCP sends discover packets when retrying to gain an IP address, the transaction ID is unique for each request instead of showing the transaction it is applicable to.	—
GT3K-10297	DHCP request interval uses a randomized exponential back off instead of using the exact configured value.	—

1.2.6. Precision Time Protocol

The following table lists the known issues with the precision time protocol input or output. Including all known issues with PTP profile implementation.

Table 1-6. Known Issues: Precision Time Protocol Input or Output

Issue Reference	Known Issue	Workaround
GT3K-5205	When a port is configured to be an ITU-T G.8265.1 timeReceiver, it accepts and synchronizes to a device reporting QL-INV (Invalid Quality Level).	—
GT3K-5210	The leap second indicator in the PTP announce message clears, one second before the leap second event actually occurs.	—
GT3K-5323	The IEEE® C37.238-2011 and IEEE C37.238-2017 TLVs indicate a better clock accuracy than the actual calculated inaccuracy.	—
GT3K-5734	In the “Server Force Quality (Option II)” drop down list, the option for QL-ST3 is missing.	—
GT3K-5741	PTP G.8265.1 timeReceiver occasionally fails to renew unicast peer subscription after re-enabling peer.	Disable then re-enable the unicast peer a second time in the CMT.
GT3K-5744	Incorrect clock class of 102 is reported when in holdover using ITU-T G.8265.1 TimeTransmitter with Option 1 (E1) selected.	—
GT3K-5745	The SSM outputs are not aligned between the T1 Output and the ITU-T G.8265.1 (Option II) output when the clock is synchronized or in Holdover state.	—
GT3K-5747	The GridTime™ 3000 GNSS Time Server when operating as a ITU-T G.8265.1 timeReceiver waits too long to retry after receiving a denial response.	—
GT3K-10260	The GridTime 3000 GNSS Time Server synchronizes to a upstream PTP GM that is reporting an accuracy of 0xFE (Unknown).	—

Table 1-6. Known Issues: Precision Time Protocol Input or Output (continued)

Issue Reference	Known Issue	Workaround
GT3K-10270	In the E2E PTP profile, the delay request message transmitted by the client is not received according to the user-specified configuration.	—
GT3K-10295	When the ATOI displayName value is longer than 10 characters, it fails to display in Wireshark or other packet capture tool.	—
GT3K-10309	Changing of the Local port priority values on one of the two PTP qualified inputs is not changing input from one PTP source to another.	—
GT3K-10313	Maximum inaccuracy threshold differs from reported clock inaccuracy by 14 ns.	
GT3K-10316	PTP Delay response receipt timeout threshold does not consistently apply 2× delay request interval.	
GT3K-10317	TimeReceiver only port incorrectly Reports "Passive" Port State.	
GT3K-10355	ATOI TLV currentOffset, jumpSeconds and timeOfNextJump updated a second late at DST rollover.	—
GT3K-10384	TimeTraceable Flag incorrectly sets to False in Holdover states.	—

1.2.7. Network Time Protocol

The following table lists the known issues with Network Time Protocol input and output implementation.

Table 1-7. Known Issues: Network Time Protocol Related Issues

Issue Reference	Known Issue	Workaround
GT3K-2826	NTP multicast and broadcast rates are not aligned to the nearest second or minute. For example, if configured for one minute, the packets are not aligned to the nearest minute.	—
GT3K-10380	NTP Multicast IP address validation allows invalid loopback address 127.0.0.0.	—
GT3K-10381	NTP Client sets reference ID to "GPS" without GNSS synchronization.	—

1.2.8. Parallel Redundancy Protocol

The following table lists the known issues with the parallel redundancy protocol implementation.

Table 1-8. Known Issues: Parallel Redundancy Protocol Implementation

Issue Reference	Known Issue	Workaround
GT3K-4622	When a timing port is removed from a PRP pair, the old PRP-B port LED turns on when a cable is connected to the PRP-A port.	—

1.2.9. Synchronous Ethernet (SyncE)

The following table lists the known issues with the SyncE functions and its implementations.

Table 1-9. Known Issues: SyncE Functionality and Validation Issues

Issue Reference	Known Issue	Workaround
GT3K-10240	When the oscillator tune range has been exceeded, the clock does not deselect the SyncE source.	—
GT3K-10301	When linked at 10M or 100M half-duplex, the copper Ethernet ports emits the ESMC messages.	—

Table 1-9. Known Issues: SyncE Functionality and Validation Issues (continued)

Issue Reference	Known Issue	Workaround
GT3K-10302	SyncE Wander Transfer Gain Peaking exceeds ITU-T G.8262 Recommended Limit	—
GT3K-10314	Output suppression behaviors are inconsistent with the configured suppression settings.	—
GT3K-10393	Excessive ESMC messages received on one port causes syntonization loss on the other port.	—

1.2.10. T1/E1/J1

The following table lists the known issues with T1/E1/J1 outputs.

Table 1-10. Known Issues: T1/E1/J1

Issue Reference	Known Issue	Workaround
GT3K-3023	When T1 or J1 is configured, the Idle Data Link sequence is not seen when SSM is disabled.	—
GT3K-10294	When configured for Modified CRC Multiframe format, the GridTime 3000 emits a framed E1 outputs of all 1s.	—

1.2.11. DCLS IRIG-B and AM IRIG-B

The following table lists the known issues with DCLS IRIG-B or AM IRIG-B.

Table 1-11. Known Issues: DCLS IRIG-B and AM IRIG-B

Issue Reference	Known Issue	Workaround
GT3K-3015	When two IRIG-B inputs are present and one has better quality than the other, the device does not switch to use the better of the two sources.	—
GT3K-3016	When two IRIG-B inputs with equal quality are present, the device toggles between each source.	—
GT3K-10382	IRIG-B reports invalid time accuracy in "Time Unknown, Frequency Only" state.	—

1.2.12. Serial String

The following table lists the known issues with the RS232 and RS422 serial string outputs.

Table 1-12. Known Issues: Serial String

Issue Reference	Known Issue	Workaround
GT3K-10306	NMEA ZDA Serial String does not report Local Offset with Daylight Saving offset when DST enabled.	—

1.2.13. Logging

The following table lists the known issues with the device log file generation.

Table 1-13. Known Issues: Alarm Generations or Conditions

Issue Reference	Known Issue	Workaround
GT3K-10248	No log events are generated in some events where a password has failed to be set. - When a password does not meet the requirements - When the current password is incorrect - When the current and new passwords match - When the confirmed password does not match with the new password - When an admin changes a user's password - When a user tries to reuse the same password	—

1.2.14. Alarms

The following table lists the known issues with the device alarm generation or conditions.

Table 1-14. Known Issues: Alarm Generations or Conditions

Issue Reference	Known Issue	Workaround
GT3K-5295	When the device reports an IRIG-B input alarm (No Input or Invalid Input) and the device is power cycled, the alarms and notifications do not reappear.	—
GT3K-10385	The "No IRIG-B Input Signal" alarm remains active after disabling the IRIG-B input port.	—

1.2.15. Global Navigation Satellite System (GNSS)

The following table lists the known issues with GNSS.

Table 1-15. Known Issues: GNSS

Issue Reference	Known Issues	Workaround
GT3K-10275	Disabling all GNSS constellations in the configuration file do not disable GNSS and continues to stay locked to all previously configured constellations.	—
GT3K-10311	GNSS commissioning log reports the excessive height value for zero elevation.	—

1.3. Resolved Issues

This section describes the resolved issues in the release version 1.2r0.0.

1.3.1. Additional Device Functions

The following table lists the resolved issues with the general function of the device, including any issues related to output suppression, daylight savings rollover, licenses, or expansion oscillator usage.

Table 1-16. Resolved Issues: General Functions of the Device

Issue Reference	Resolved Issue
GT3K-2984	The second alarm page on the LCD is now readable with more than 7 active alarms.
GT3K-4420	Increased threshold for alternate source selection after previously being in test mode to prevent persistent switching of in and out of sync states when coming into sync with GNSS.
GT3K-5834	Implemented rate limiting on the Ethernet Switch Chip to prevent the switch being overloaded and crashing at high NTP rates.

Table 1-16. Resolved Issues: General Functions of the Device (continued)

Issue Reference	Resolved Issue
GT3K-5572	Daylight savings time zone id updates at the same time as a daylight savings change.

1.3.2. Clock Management Tool (CMT)

The following table lists the resolved issues with the clock management tool, including any field validation errors, and issues with any buttons or configurable options.

Table 1-17. Resolved Issues: Clock Management Tool (CMT)

Issue Reference	Resolved Issue
GT3K-2464	When the user has a read only permission set, they are not prompted to save when navigating away from a configuration page.
GT3K-2735	Updated the invalid error message for the Network Name field to describe what characters are allowed.
GT3K-2805	Removed NTP Reserved/Off. It is recommended to "Disable NTP Traffic" instead.
GT3K-2929	Session token expirations have been changed to use an in browser counter instead of relying on the clock's internal time, ensuring that when the Test mode is configured, it does not automatically log the user out.
GT3K-2930	The IPv4 static gateway and netmask are reordered to be consistent with the standard IPv4 configuration settings.
GT3K-3048	The CMT displays the C37.238 TLV outgoing setting for both end-to-end and peer-to-peer options, when it was previously hidden.
GT3K-4309	Removed numeric controls from IP address input fields.
GT3K-5252	The CMT loads correctly when a new user is logs in for the first time.
GT3K-5262	The GNSS coordinates are no longer shown when GNSS is disabled.
GT3K-5325	Changed the Authentication module so that new local login providers are unable to be created, and to prevent the default local provider from being deleted.
GT3K-5327	The GUID of a user is no longer displayed when attempting to delete a user.
GT3K-5623	The Sky plot displayed on the CMT dashboard now correctly shows that 90-degree elevation in the center of the diagram instead of the edge.
GT3K-5822	Underscore is added to the allowable special characters for passwords.
GT3K-5871	The antenna cable delays boundary input ranges have been changed to have a min value of -32000 and a max value of 32000.
GT3K-10187	The Elevation and Azimuth values displayed on the GNSS Sky Chart labels on the CMT dashboard have been removed.
GT3K-10233	"Active Oscillator" on the CMT dashboard is renamed to "Oscillator".
GT3K-10262	Clicking on the Microchip logo when in the authentication module redirects the user to the top-level page in the authentication module.

1.3.3. Security and Authentication

The following table lists the resolved issues with the authentication of users through a local or an external authentication provider and any issues with access control.

Table 1-18. Resolved Issues: Authentication and Access Control Related Issues

Issue Reference	Resolved Issue
GT3K-3408	When GridTime 3000 GNSS Time Server is configured to use RADIUS, Access-Request messages sent by the GridTime 3000 GNSS Time Server contains the NAS-Identifier or NAS-IPAddress attributes.
GT3K-3432	RADIUS Access Request message Id is no longer always 0 and instead uses randomized identifiers.
GT3K-4596	Fixed issue where device occasionally required two CMT login attempts.
GT3K-5635	Javascript Web Tokens (JWT) expire after a user has logged out preventing the reuse of token to gain access to the device.

Table 1-18. Resolved Issues: Authentication and Access Control Related Issues (continued)

Issue Reference	Resolved Issue
GT3K-5757	Amended the error message that is displayed to a user if they try to log in to the device if they have been locked out.
GT3K-5758	Changed the "Number of failed attempt setting" counter to start at 1 not 0 .
GT3K-5827	When a user is deleted, the session ends immediately. Note: The user is redirected back to the login page once the browser has been refreshed.
GT3K-10246	A httpOnly cookie is added for storage of the session token to prevent cross site scripting, exposing the token.
GT3K-10250	
GT3K-10253	Santization is added to the redirectURL to prevent injection of Javascript into the window.location.href fields.
GT3K-10283	Certificate Signing Requests (CSR) contain a field for IP address and DNS.
GT3K-10397	Reworked login failure messages to remove user enumeration.
GT3K-10398	Web server information is no longer displayed in the HTTP header.
GT3K-10399	In-secure cryptographic ciphers for TLS are removed.

1.3.4. Simple Network Management Protocol (SNMP)

The following table lists the resolved issues with SNMP including any issues with SNMP authentication, SNMP traps or SNMP configuration.

Table 1-19. Resolved Issues: SNMP

Issue Reference	Resolved Issue
GT3K-2880	Input validation is in place for <code>gt3kIPv4CurrentAddress</code> , <code>gt3kNTPMulticastIPv4Address</code> , <code>gt3kNTPPeerIPv4Address</code>
GT3K-2891	"None (13)" is available as an option in <code>gt3kSERIALString</code>
GT3K-2948	Single response returned for "getnext" request on <code>ieeeC37238TimePropDSLocalTCurOfs.0</code> and <code>ieeeC37238TimePropDSUTCOfstNext</code> variables as expected.
GT3K-5301	The specific-trap identifier in SNMPv1 extracts the value from the OID.
GT3K-5564	Input validation is in place for <code>gt3kSNMPSubscriptionIPAddress</code>
GT3K-5764	The GNSSMaskAngle is moved to be in the GNSS configuration table instead of the GNSS status table.
GT3K-5766	<code>gt3kHardwareVoltage</code> is removed due to no information being populated.
GT3K-10204	Input validation is in place for <code>gt3kProgrammablePulseDuration</code> .
GT3K-10205	Input validation is in place for <code>gt3kAdminDHCPPreferredAddress</code> .
GT3K-10206	Input validation is in place for <code>gt3kTimingDHCPPreferredAddress</code> .
GT3K-10207	Input validation is in place for <code>gt3kAdminLinkLocPreferredAddress</code> .
GT3K-10208	Input validation is in place for <code>gt3kTimingLinkLocalPreferredAddress</code> .
GT3K-10209	Input validation is in place for <code>gt3kPTPPeerIPv4Address</code> .
GT3K-10210	Input validation is in place for <code>gt3kNTPPeerIPv4Address</code> .
GT3K-10211	Input validation is in place for <code>gt3kNTPMulticastIPv4Address</code> .
GT3K-10212	Input validation is in place for <code>gt3kSNMPSubscriptionsIPAddress</code> .
GT3K-10213	Input validation is in place for <code>gt3kSYSLOGSubscriptionsIPAddress</code> .
GT3K-10244	SNMP SET actions are allowed when the community string is set to "public". Previous behavior prevents SET actions when the string was set to "public".

1.3.5. Networking

The following table lists the known issues with the network ports including both the administrator and timing ports, their interfacing protocols and behavior.

Table 1-20. Resolved Issues: Networking Related Issues

Issue Reference	Resolved Issues
GT3K-3049	Link status reporting in CMT dashboard and SNMP (<code>gt3kNETWORKLinkStatus</code>) for timing ports map to the actual state of the port.
GT3K-5321	When reverting back to a link-local address, ARP requests are not sent to 0.0.0.0.

1.3.6. Precision Time Protocol

The following table lists the known issues with the precision time protocol input or output, including all known issues with PTP profile implementation.

Table 1-21. Resolved Issues: Precision Time Protocol Input or Output

Issue Reference	Resolved Issue
GT3K-2896	IEEE® C37.238-2017 “Default Domain field” enforces the correct limits (0–127 and 254).
GT3K-2906	Possible to set the “Require on incoming” for ATOI separately from C37.238.
GT3K-2921	When the clock is a ITU-T G.8275.1 timeTransmitter, it report an <code>offsetScaledLogVariance</code> of 65535 when in holdover instead of 20061.
GT3K-2945	Updated the allowable range for Request Announce Interval for ITU-T G.8265.1 client peer configuration to match the range specified in G.8265.1.
GT3K-3048	E2E/P2P “timeTransmitter Only” mode shows “C37.238 TLV Outgoing: False” settings.
GT3K-3049	Changing IP address of ITU-T G.8265.1 peer stops requests to previous address without requiring a restart.
GT3K-3054	ITU-T G.8265.1 output reflects a true <code>frequencyTraceable</code> flag when the GridTime 3000 is synchronized to a <code>frequencyTraceable</code> PTP input.
GT3K-4436	The ITU-T G.8265.1 Server force quality setting is removed from ITU-T G.8265.1 client options as they are not required.
GT3K-5577	When receiving a PTP input on L3 with “transportSpecific hardwareCompatibility” set, the GridTime™ 3000 GNSS Time Server pads the output as required by IEEE 1588-2008.
GT3K-5614	Validation is added to PTP unicast pair IP address settings to prevent the use of an invalid IP address.
GT3K-5767	When operating as a timeReceiver, the GridTime 3000 GNSS Time Server correctly selects a higher priority PTP timeReceiver when there are multiple timeTransmitters announcing.
GT3K-5843	The PTP <code>frequencyTraceable</code> flag correctly indicates traceability to a frequency source.
GT3K-10222	When configured as a ITU-T G.8265.1 timeTransmitter with Server Networking Option to E1, this reports <code>clockClass</code> based on the quality level mapping.

1.3.7. Network Time Protocol

The following table lists the resolved issues with the network time protocol input and output implementation.

Table 1-22. Resolved Issues: Network Time Protocol

Issue Reference	Resolved Issue
GT3K-2877	NTP advanced setting “NTP Default Passkey” enforces an input limit range between 1 – 8, in the CMT.
GT3K-2881	When configuring an NTP client, the “Server IP address” allows the IP address to match the IP address of the clock’s NTP client port.
GT3K-3942	The NTP polling time is saved between power cycles.
GT3K-5292	The server IP of an NTP client is saved when the server IP address is updated while transmitting NTP.

1.3.8. Parallel Redundancy Protocol

The following table lists the resolved issues with the parallel redundancy protocol implementation.

Table 1-23. Resolved Issues: Parallel Redundancy Protocol Implementation

Issue Reference	Resolved Issues
GT3K-4356	Amended behavior of PRP port pairs and their associated alarms and LED link states.
GT3K-4359	When PRP is enabled on two ports, and there are no cables connected. The “PRP Link Failure” alarm appears.

1.3.9. T1/E1/J1

The following table lists the resolved issues with the T1/E1/J1 implementation.

Table 1-24. Resolved Issues: Network Time Protocol

Issue Reference	Resolved Issue
GT3K-2324	T1/E1 automatically becomes available after the license is applied. Note: There may be a small delay between applying the license and the ports appearing. It is recommended to give the GridTime 3000 approximately one minute to make this change.
GT3K-2868	The CMT displays that waveform shaper settings on port T1/T2 when J1 is selected.
GT3K-10054	T1/E1 and Fixed Frequency show when the license is not installed.
GT3K-10221	When SSM override is disabled and SSM Bits are enabled, the GridTime 3000 sends valid SSM codes.

1.3.10. Serial String

The following table lists the resolved issues with the RS232 and RS422 serial string implementation.

Table 1-25. Resolved Issues: Serial String

Issue Reference	Resolved Issues
GT3K-5542	NMEA RMC string conveys position in Degree, Decimal Minute (DDM) format instead of Degrees Minutes Seconds (DMS).
GT3K-5570	Serial String B, D and E report worst possible quality instead of estimating quality once the device has gone out-of-sync.

1.3.11. Logging

The following table lists the resolved issues with the device log file generation.

Table 1-26. Resolved Issues: Logging

Issue Reference	Resolved Issue
GT3K-5362	The severity level for GNSS Log Generation Descheduled is changed from 4 to 5.
GT3K-5369	The Log content (priority, severity and Message ID) for IRIG Output Signal Unsuppressed is updated.
GT3K-5372	The Log content (severity, Message ID and user) for Password Update Failure is updated.
GT3K-5384	MSG Id for No IRIG-B Input Log entry to IRIG and changed severity from critical to warning.
GT3K-5399	GridTime 3000 logs when a unicast peer or SNMP subscription is created or deleted.
GT3K-5527	A log entry creates an independent log entry when a role is created and when a role is changed.
GT3K-5586	A log entry is sent when the Test mode is disabled.
GT3K-5641	A log entry is sent when an SFP is disconnected.
GT3K-5749	IRIG-B Output related events are no longer have a hard-coded process ID and use the boot count instead.
GT3K-5750	IRIG-B Start and Stop Logs are triggered when enabling AM IRIG-B.
GT3K-5754	Structured data that includes the “Role” element (for example, Password updates, user log in and out) shows the correct role based on what role group the user belongs to.

The log entries being generated in the log files are simplified for improving readability by removing unnecessary structured data elements.

1.3.12. Alarms

The following table lists the resolved issues with the device alarm generation or conditions.

Table 1-27. Resolved Issues: Alarm Generations or Conditions

Issue Reference	Resolved Issue
GT3K-2524	Corrected an issue where the VIRIG alarm was not triggered when IRIG input without C37 was applied.
GT3K-5307	When an address collision is detected, an "Address Collision" alarm is successfully sent.
GT3K-10217	A "No IRIG Input" alarm is present for each IRIG-B input port independently.

1.3.13. Global Navigation Satellite System (GNSS)

The following table lists the resolved issues with GNSS

Table 1-28. Resolved Issues: GNSS

Issue Reference	Resolved Issue
GT3K-4634	The stability of the Beidou and Galileo constellations is improved if these are used without GPS or GLONASS.
GT3K-5708	Added validation to the GNSS Antenna Cable Delay fields in the CMT and SNMP to match manufacturers specifications and prevent an integer rollover.
GT3K-4451 and GT3K-5844	Beidou B1 and Beidou enable/disable settings are combined to allow enabling/disabling of the Beidou constellation. Previous behavior provided configuration options that would not change any configuration in the device.

2. Upgrading the Firmware

This section describes how to upgrade the GridTime 3000 firmware.

2.1. Upgrading the Firmware

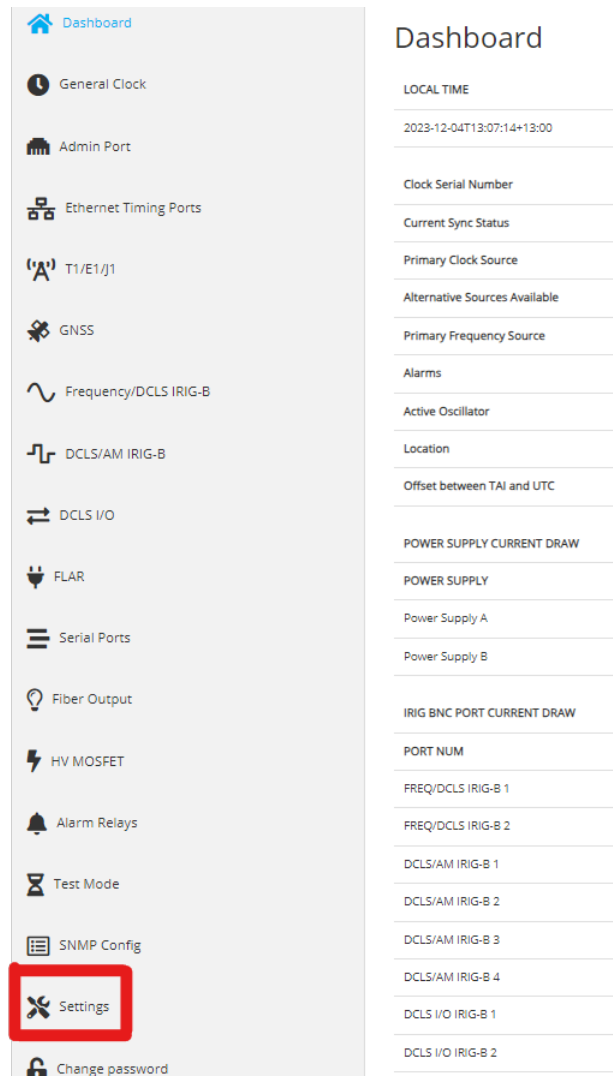
This section describes how to upgrade the GridTime 3000's firmware using the CMT. The CMT is built into the device and can be accessed by navigating to either of the IP addresses on the LCD using a web browser.

Note: Only an administrator user can upgrade the GridTime 3000's firmware.

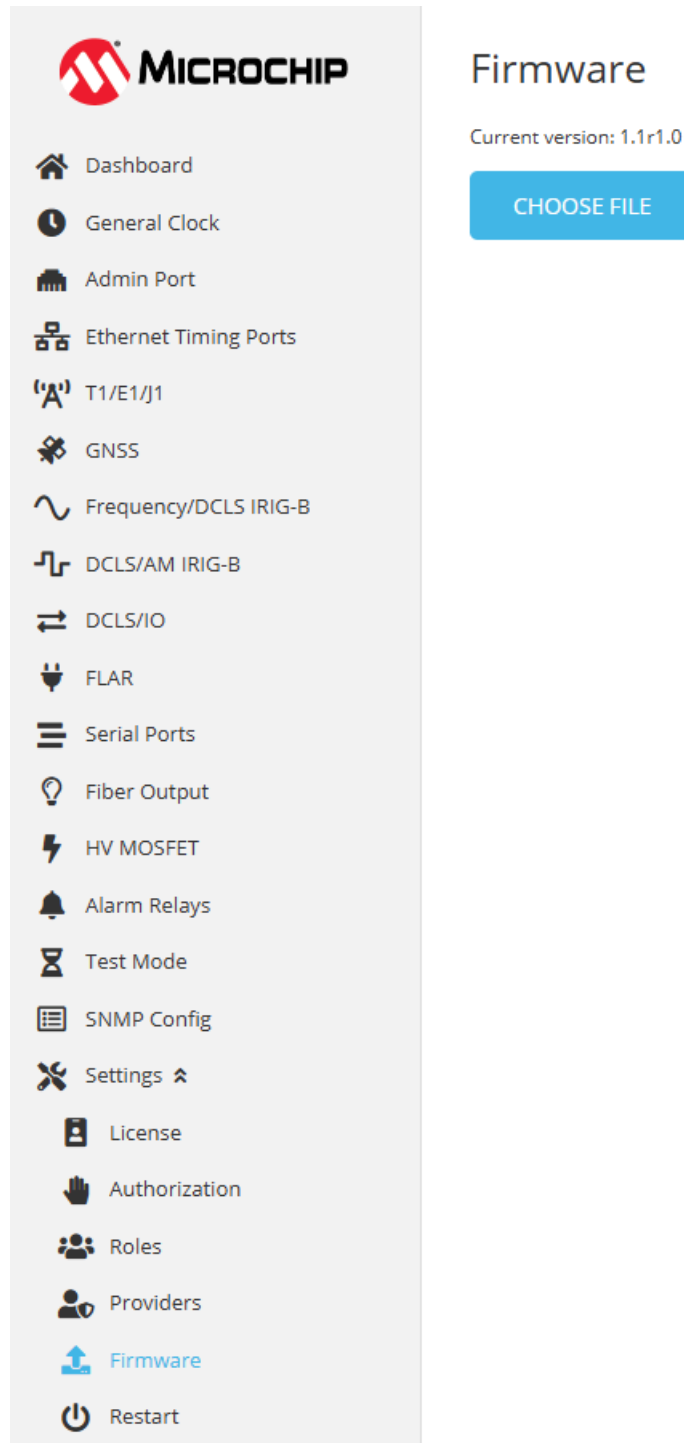
To upgrade the firmware, perform the following steps:

1. Log in to the CMT as an administrator user.
2. On the left navigation pane of the CMT Dashboard screen, click **Settings** and then click **Firmware**. This opens the Firmware window.

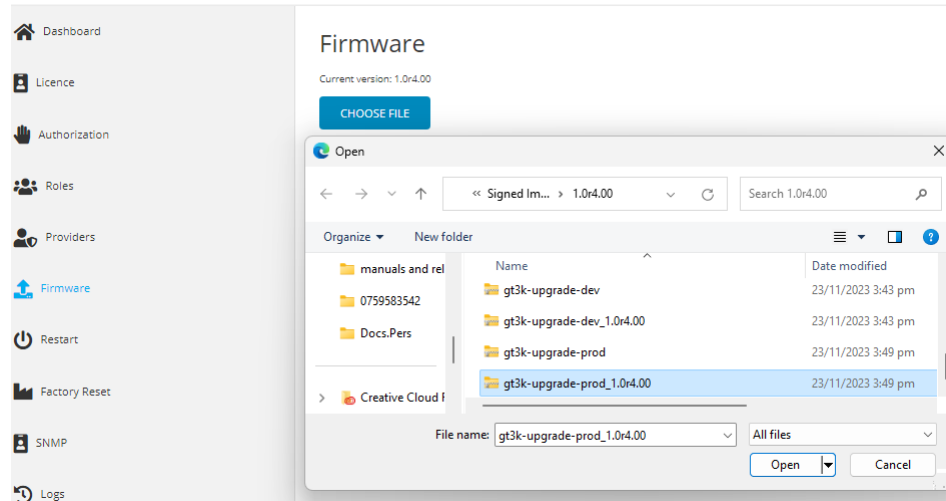
Figure 2-1. CMT Dashboard



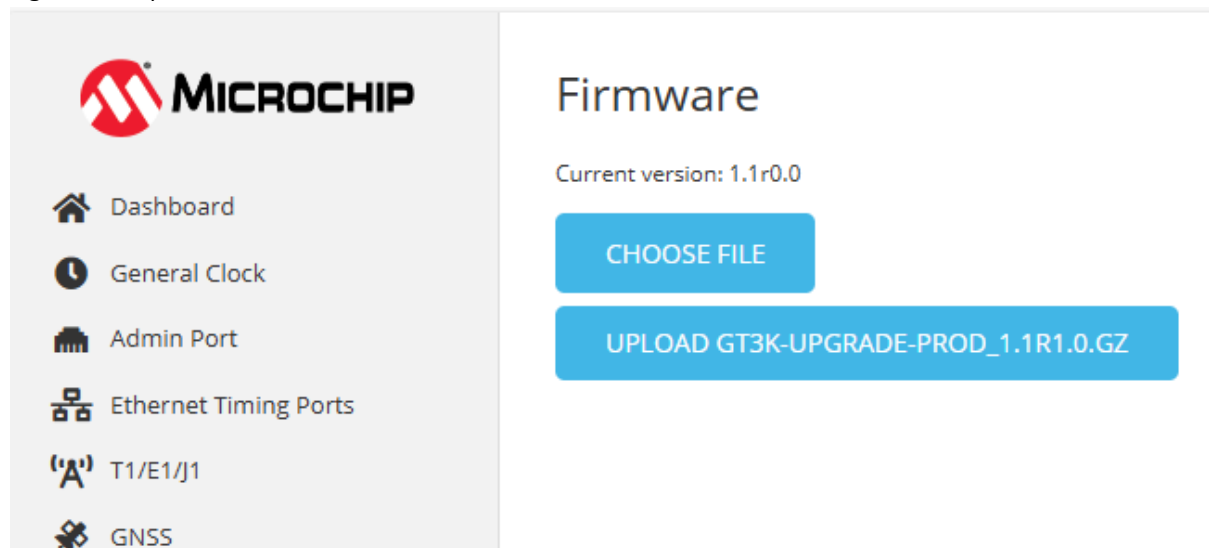
3. To select the new firmware image, click **CHOOSE FILE**. This opens the **Open** dialog box.

Figure 2-2. Firmware Window

4. From the **Open** dialog box, locate the file on your system, click on the image, and then click the **Open** button.

Figure 2-3. Locate Firmware

5. An **UPLOAD [Firmware Image]** button appears. Click this button to upload the new firmware image to the device. The upload tracking percentage of the image to the device is displayed.

Figure 2-4. Upload New Firmware

6. Once the progress reaches 100%, an **APPLY FIRMWARE UPDATE** button appears. Click this button to upload the device's firmware.

Figure 2-5. Apply Firmware

Firmware

Current version: 1.1r0.0

APPLY FIRMWARE UPDATE

Update

7. An **INSTALLING PLEASE WAIT...** message appears and the GridTime 3000 reboots.

Figure 2-6. Install Firmware

Firmware

Current version: 1.0r4.00

INSTALLING PLEASE WAIT...

8. If the upgrade is successful, then the device shows the new firmware on its LCD during boot up and in the firmware tab of the CMT, once you have logged out and then logged back in. If the firmware version remains the same, this indicates a potential upgrade failure. Retry the upgrade and if the upgrade failure persists, contact Microchip technical support.

3. Contacting Technical Support

If you encounter any difficulty installing the update or operating the product, contact Microchip Frequency and Time Division (FTD) Services and Support at:

Region	Address	Contact Information
USA Call Center: Including Americas, Asia and Pacific Rim	Microchip FTD Services and Support 3870 N. First Street San Jose, CA 95134	- Toll-free in North-America: 1-888-367-7966 - Telephone: 408-428-7907 - E-mail: SJO-FTD.Support@microchip.com - Website: www.microchip.com/en-us/products/synchronization-and-timing-systems
Europe, Middle East, and Africa (EMEA) Call Center	Microchip FTD Services and Support EMEA Altlaufstrasse 42 85635 Hoehenkirchen-Siegersbrunn Germany	- Telephone: +49 700 3288 6435 - Fax: +49 8102 8961 533 - E-mail: FTD.EMEA.Support@microchip.com FTD.EMEA_sales@microchip.com - Website: microchipsupport.force.com/s/
Australia and New Zealand	Tekron International Ltd. Level 1, 47 The Esplanade Lower Hutt, 5022 New Zealand	- Telephone: +64 4 566 7722 - Email: nzp-support@microchip.com

4. References

- *GridTime™ 3000 GNSS Time Server SRN* (this document)
- *GridTime™ 3000 GNSS Time Server Installation Manual*(DS00004572)
- *GridTime™ 3000 SNMP MIB*

This SRN and the User Guide are provided in PDF format. The SNMP MIB is provided as an ASCII text file.

Note: To view and print PDFs, download Adobe Acrobat Reader from get.adobe.com/reader/.

5. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Table 5-1. Revision History

Revision	Date	Description																						
G	06/2026	The following is the list of changes made in revision G of this document: • Updated the new features in release 1.2r0.0 • Updated the resolved and known issues sections. The following issues were removed due to re-evaluation of issue criteria or found to not be issues. <table><tr><th>Issue Number</th><th>Issue Number</th></tr><tr><td>GT3K-2491</td><td>GT3K-3075</td></tr><tr><td>GT3K-2516</td><td>GT3K-3076</td></tr><tr><td>GT3K-2606</td><td>GT3K-3277</td></tr><tr><td>GT3K-2730</td><td>GT3K-4418</td></tr><tr><td>GT3K-2768</td><td>GT3K-4522</td></tr><tr><td>GT3K-2879</td><td>GT3K-5252</td></tr><tr><td>GT3K-2881</td><td>GT3K-5305</td></tr><tr><td>GT3K-2911</td><td>GT3K-5595</td></tr><tr><td>GT3K-2919</td><td>GT3K-5756</td></tr><tr><td>GT3K-3051</td><td></td></tr></table>	Issue Number	Issue Number	GT3K-2491	GT3K-3075	GT3K-2516	GT3K-3076	GT3K-2606	GT3K-3277	GT3K-2730	GT3K-4418	GT3K-2768	GT3K-4522	GT3K-2879	GT3K-5252	GT3K-2881	GT3K-5305	GT3K-2911	GT3K-5595	GT3K-2919	GT3K-5756	GT3K-3051	
Issue Number	Issue Number																							
GT3K-2491	GT3K-3075																							
GT3K-2516	GT3K-3076																							
GT3K-2606	GT3K-3277																							
GT3K-2730	GT3K-4418																							
GT3K-2768	GT3K-4522																							
GT3K-2879	GT3K-5252																							
GT3K-2881	GT3K-5305																							
GT3K-2911	GT3K-5595																							
GT3K-2919	GT3K-5756																							
GT3K-3051																								
F	03/2025	The following is the list of changes made in revision F of this document: • Updated the new feature in release 1.1r1.0 • Updated the Upgrading firmware section. • Updated the Known Issues > Simple Network Management Protocol (SNMP) section Table 5-2. Removed the following issues due to re-evaluation of issue criteria. <table><tr><th>Issue Number</th></tr><tr><td>GT3K-2191</td></tr></table>	Issue Number	GT3K-2191																				
Issue Number																								
GT3K-2191																								
E	02/2025	The following is the list of changes made in revision E of this document: • Updated the Upgrading firmware section. • Updated the Resolved and known Issues Section.																						
D	09/2024	The following is the list of changes made in revision D of this document: • Updated the document for release v1.1r.0. • Added the Resolved and known Issues Section. • Updated the Upgrading Firmware section. Table 5-3. Removed the following issues due to re-evaluation of issue criteria. <table><tr><th>Issue Number</th><th>Issue Number</th></tr><tr><td>GT3K-2486</td><td>GT3K-4446</td></tr><tr><td>GT3K-4265</td><td>GT3K-4653</td></tr><tr><td>GT3K-4362</td><td>GT3K-4519</td></tr></table>	Issue Number	Issue Number	GT3K-2486	GT3K-4446	GT3K-4265	GT3K-4653	GT3K-4362	GT3K-4519														
Issue Number	Issue Number																							
GT3K-2486	GT3K-4446																							
GT3K-4265	GT3K-4653																							
GT3K-4362	GT3K-4519																							

Table 5-1. Revision History (continued)**Table 5-4.** Removed the following issues due to re-evaluation of issue criteria. (continued)

Revision	Date	Description																																																
C	02/2024	The following is the list of changes made in revision C of the document: • Updated the document for release v1.0r4.0. • Added the Resolved and known Issues Section. • Updated the Upgrading Firmware section. Table 5-4. Removed the following issues due to re-evaluation of issue criteria. <table><tr><th>Issue Number</th><th>Issue Number</th><th>Issue Number</th><th>Issue Number</th></tr><tr><td>GT3K-2317</td><td>GT3K-2936</td><td>GT3K-2985</td><td>GT3K-3427</td></tr><tr><td>GT3K-2486</td><td>GT3K-2939</td><td>GT3K-2994</td><td>GT3K-3431</td></tr><tr><td>GT3K-2592</td><td>GT3K-2949</td><td>GT3K-2998</td><td>GT3K-4205</td></tr><tr><td>GT3K-2594</td><td>GT3K-2958</td><td>GT3K-3002</td><td>GT3K-4215</td></tr><tr><td>GT3K-2668</td><td>GT3K-2960</td><td>GT3K-3005</td><td>GT3K-4218</td></tr><tr><td>GT3K-2669</td><td>GT3K-2968</td><td>GT3K-3032</td><td>GT3K-4265</td></tr><tr><td>GT3K-2701</td><td>GT3K-2973</td><td>GT3K-3038</td><td>GT3K-4433</td></tr><tr><td>GT3K-2740</td><td>GT3K-2974</td><td>GT3K-3039</td><td>GT3K-4446</td></tr><tr><td>GT3K-2741</td><td>GT3K-2978</td><td>GT3K-3040</td><td>GT3K-4451</td></tr><tr><td>GT3K-2934</td><td>GT3K-2982</td><td>GT3K-3044</td><td>GT3K-4515</td></tr><tr><td>GT3K-3423</td><td></td><td>GT3K-4360</td><td></td></tr></table>	Issue Number	Issue Number	Issue Number	Issue Number	GT3K-2317	GT3K-2936	GT3K-2985	GT3K-3427	GT3K-2486	GT3K-2939	GT3K-2994	GT3K-3431	GT3K-2592	GT3K-2949	GT3K-2998	GT3K-4205	GT3K-2594	GT3K-2958	GT3K-3002	GT3K-4215	GT3K-2668	GT3K-2960	GT3K-3005	GT3K-4218	GT3K-2669	GT3K-2968	GT3K-3032	GT3K-4265	GT3K-2701	GT3K-2973	GT3K-3038	GT3K-4433	GT3K-2740	GT3K-2974	GT3K-3039	GT3K-4446	GT3K-2741	GT3K-2978	GT3K-3040	GT3K-4451	GT3K-2934	GT3K-2982	GT3K-3044	GT3K-4515	GT3K-3423		GT3K-4360	
Issue Number	Issue Number	Issue Number	Issue Number																																															
GT3K-2317	GT3K-2936	GT3K-2985	GT3K-3427																																															
GT3K-2486	GT3K-2939	GT3K-2994	GT3K-3431																																															
GT3K-2592	GT3K-2949	GT3K-2998	GT3K-4205																																															
GT3K-2594	GT3K-2958	GT3K-3002	GT3K-4215																																															
GT3K-2668	GT3K-2960	GT3K-3005	GT3K-4218																																															
GT3K-2669	GT3K-2968	GT3K-3032	GT3K-4265																																															
GT3K-2701	GT3K-2973	GT3K-3038	GT3K-4433																																															
GT3K-2740	GT3K-2974	GT3K-3039	GT3K-4446																																															
GT3K-2741	GT3K-2978	GT3K-3040	GT3K-4451																																															
GT3K-2934	GT3K-2982	GT3K-3044	GT3K-4515																																															
GT3K-3423		GT3K-4360																																																
B	11/2022	The following is the list of changes made in revision C of the document: • Updated the document for release v1.0r1.0. • Updated the New Features in v1.0r1.0 section. • Updated the Additional Device Functions section. • Added the Authentication section. • Updated the Upgrading Firmware section.																																																
A	10/2022	Initial Revision																																																

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at <https://www.microchip.com/en-us/about/legal-information/microchip-trademarks>.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.