Iris Operations, Administration, and Maintenance Guide

Version 7.13.2

Tektronix communications

Copyright

Tektronix Communications
3033 W President George Bush Highway
Plano, TX 75075 USA
+1 469-330-4000 (voice)
www.tekcomms.com

992-0415-08-001-140228

Customer Support

Plano, Texas USA - serves North America, South America, Latin America
+1 469-330-4581 (Customer Support voice)
uaservice@tek.com (Customer Support USA email)

London, England UK - serves Northern Europe, Middle East, and Africa
+44-1344-767-100 (Customer Support voice)
uaservice-uk@tek.com (Customer Support UK email)

Frankfurt, Germany DE - serves Central Europe and Middle East
+49-6196-9519-250 (Customer Support voice)
uaservice-de@tek.com (Customer Support DE email)

Padova, Italy IT - serves Southern Europe and Middle East
+39-049-762-3832 (Customer Support voice)
uaservice-it@tek.com (Customer Support IT email)

Melbourne, Australia - serves Australia
+61-396-330-400 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Singapore - serves Asia and the Pacific Rim
+65-6356-3900 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Table of Contents

What's New in Admin 7.13.2?

Feature ID	Description	Section
F-02250	**SIP Message with SMS Full Content Stored Short-term** This feature enables full SMS payload content, within SIP messages, to be stored in the G10 probe for a short-term duration and is only visible with the PA and ISA application. This allows PA and ISA users to see all SMS content for troubleshooting purposes. SMS Full Content Enabled is a per probe option, and is set on the Probe Monitoring Details tab.	Monitoring Details tab SMS Full Content Enabled - System Impact
F-02387	**Iris 3G GeoSoft** With this feature, you will be able to utilize the virtual GeoSoft RAN soft probe for 3G UMTS (IU) and UTRAN (Iub/Iur) monitoring. Iris ISA is now capable of showing UMTS core to UTRAN access networks in a single call trace. GeoSoft RAN 3G also provides a RAN Intelligency Feed (RIF) for geolocation vendors. This enhanced xDR feed includes RAN statistics and measurement reports required for RAN optimization use cases.	Configuring GeoSoft RAN Probes
F-02403	**Remove Selection of Protocol List from ITA** The protocol section (Edit Protocols button) has been removed from the Topology Node Details pane. ITA will determine and display known protocols observed on an ITA node. ITA will no longer require manual configuration of the list of protocols per node. This simplifies IrisView ITA node management and increases the KPI accuracy by automatically identifying all known protocols observed on a node and resulting in minimizing the “other” unknown protocol KPI.	Node Details Pane

Chapter 1 Getting Started

As an IrisView administrator you will perform a variety of tasks including, probe management, user account administration, system management, application management, software management, and alarms management. This chapter introduces you to the Iris client and server components and provides an overview of the Iris operations, administration, and maintenance tasks.

Refer to the following sections for more information:

- System Requirements
- Iris Configuration and Administration Workflow
- Accessing IrisView

Iris System Requirements

Iris Port Requirements

Contact Tektronix Communications Customer Support for a current port requirements document.

Iris Server

The Iris server provides centralized storage and management for the entire Iris system. The Iris server requests network data collected by the G10 probes and stores it in the form of statistics in a Relational Database Management System (RDBMS). Iris Clients receive data distributed from the Iris server and display this data as alarms and dashboard reports in IrisView.

Iris server functions include the following:

- Centralized storage and management of all Iris configuration data
- Alarm accumulation, distribution, and storage
- Periodic historical statistics accumulation and storage from GeoProbe G10

Communication between the G10 probes and the Iris server uses proprietary encoding; communication between the Iris server and Iris client uses HTTP/HTTPS.

The Iris server is either a Sun Sparc server or an Intel x86 that provides central control function for the GeoProbe G10 probes and the applications residing on the Iris framework. Iris server requirements vary depending on installed applications, network size, and deployed probe types. Tektronix installs and maintains the Iris server. Contact Customer Support for more information.

GeoProbe ISA Adapter Component

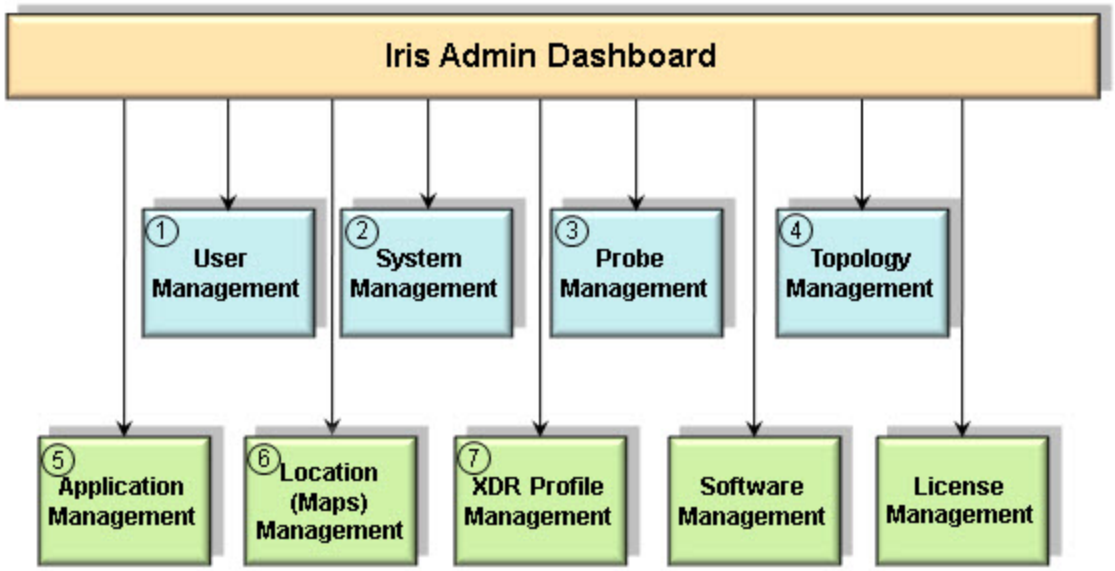
A GeoProbe ISA Adapter component is required for ISA users who have deployed GeoProbe G10s and SpIprobes. This component communicates between ISA and the GeoProbe SpIserver so that ISA can support SpIprobe data. Refer to Iris Network Data Flow for details about data flow for the ISA application.

The adapter server is designed to run on the GeoProbe SpIserver or a Sun Solaris server; customers can also utilize an existing SpIstation to run the GeoProbe ISA Adapter Component. ISA GeoProbe Adapter must always be on the same release as SpIserver.

Refer to Defining Servers for information about configuring IrisView to support the GeoProbe ISA Adapter component.

Iris Configuration and Administration Workflow

The following diagram illustrates the tasks for configuring and maintaining the Iris system and shows the Iris Admin tab you use to complete these tasks.



In a normal operational environment, the administrative tasks for managing the Iris system can be performed independent of each other. However, for first time setup, Tektronix recommends you follow these steps to ensure optimum provisioning of the Iris components.

1. Configure UUMS and administer user profiles and user access. Refer to the UUMS online help for detailed workflows and user interface descriptions.
2. Define the servers to which the Iris server communicates in the System Tab.
3. Configure G10 probes and physical device ports or configure GeoSoft RAN probes.
4. Configure topology entities: nodes, physical links, logical links, applications, protocols, entity groups.
5. Configure settings for Iris Data Storage, and ISA and ITA applications.
6. Configure Iris Maps. Define location rules for the Iris system to auto-populate entities on Iris Maps based on their names.
7. Configure XDR profiles.

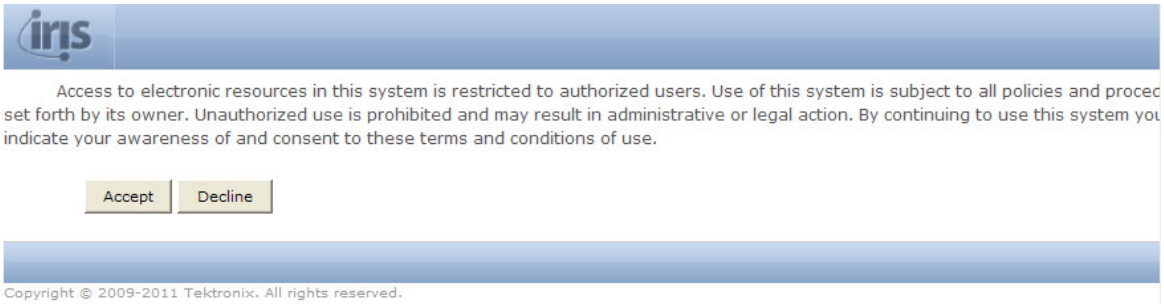
The Software tab enables you to upgrade probe software for one or more probes.

Accessing IrisView

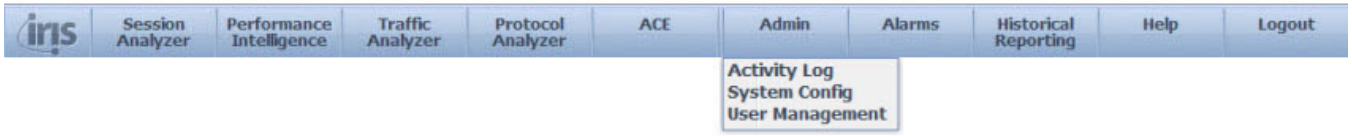
You access the Iris system using a URL defined at system install. Tektronix engineers create an Admin login for you at initial system setup for you to access the system.

If you have any problems accessing the system, contact Tektronix Customer Support.

After successful login, the advisory message appears if you configured it to appear in UUMS. Refer to the UUMS online help for details.



After clicking Accept, the IrisView toolbar appears. The toolbar enables you to navigate to and access all Iris functions using a tab-based GUI architecture.



Only purchased and licensed applications appear on the toolbar. Access to applications is controlled using Iris User Privileges. The following table describes the functionality of each toolbar button.

Session Analyzer	Launch the Iris Session Analyzer application.
Performance Intelligence	Launch the Iris Performance Intelligence application.
Traffic Analyzer	Launch the Iris Traffic Analyzer application.
Protocol Analyzer	Launch the Protocol Analyzer application.
ACE	Launch the Automated Controller Engine application.

Admin	Launch the IrisView Admin functions: System Configuration and User Management. Activity Log • View a detailed history of various user activities for Iris applications. The Activity Log is part of UUMS. System Configuration • System - configure and manage server connectivity. • Topology - configure and manage links, protocols and applications, domains, and nodes. • Applications - configure and manage store-to-disk (S2D) options, Data Record (XDR) profiles, and Iris application configuration. • Probes - configure and manage probes and physical device ports. • Locations - define rules for the Iris system to auto-populate locations on Iris Maps (latitude and longitude values) for GeoProbe and Iris nodes and probes based on their names. • Software - upload available probe application and platform packages to upgrade G10 probes. Refer to System Maintenance for more information. • Licenses - view the Iris application licenses. User Management • User Management Configuration - configure LDAP server settings, password policies and qualities for Iris LDAP, and create roles • User Management - provision user details, passwords for Iris LDAP, and assign privileges and roles
Alarms	Launch the Iris Alarms functions: • Policy Management - set alarm policy dimensions and actions. • Alarms Dashboard - monitor and view details on system generated alarms.
Historical Reporting	Launch the Historical Reporting application.
Help	Open the Iris Online Help application.
Logout	Log off and exit the system.

Chapter 2 User Management

This chapter provides an introduction to UUMS. Refer to the UUMS Online Help for more information including detailed workflows and GUI descriptions.

Unified User Management System Components

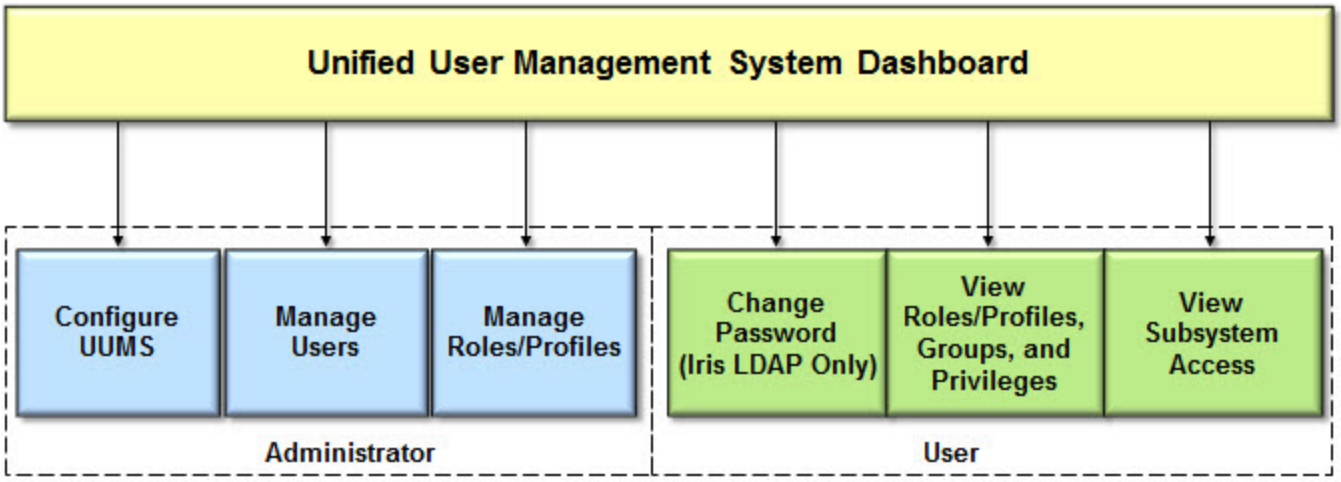
UUMS enables system administrators to perform the following tasks:

- Configure UUMS and provision user profiles and access
- Track user activities using the Activity Log

Refer to the UUMS Online Help for more information including detailed workflows and GUI descriptions.

User Management

The following graphic summarizes the User Management functions.



UUMS enables administrators to perform the following tasks:

- Configure LDAP server settings and define an Iris Admin
- Define password policies and password qualities
- Create global roles
- Configure user profiles including user ID, email address, password (for Iris LDAP), and Iris User Roles

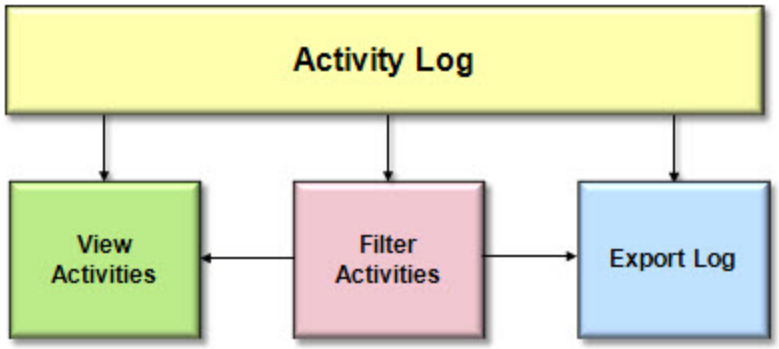
UUMS enables users to perform the following tasks:

- Change their own password (Iris LDAP)
- Verify their own user profile data
- View their currently defined roles and privileges

Activity Log

The Activity Log is a key security and audit component for the Iris system. The Activity Log provides the following features:

- Secure access to a detailed user activity history
- Filters for isolating user activity in specific areas of the system
- Export option for saving select log messages for further examination



Chapter 3 Probe Management

This chapter provides an overview of the probes used to collect data for the Iris applications and describes the Iris Network Data Flow for each application.

Refer to the following sections for additional information:

- Configuring G10 Probes
- Configuring gSoft RAN Probes
- G10 Probe Timing
- Probes Supported by Iris
- G10 Data Processing
- Iris Data Types
- Iris Network Data Flow
- Storage Maintenance
- TD140 Configuration Workflow
- TD140 Architecture Overview

Configuring G10 Probes

Probes are installed and configured at the installation site so that they can communicate with the Iris server. Once the G10 probe is physically installed, the system installer configures the probe with the IP addresses it needs to establish communications to the Iris Server for configuration and maintenance.

Once the Iris server recognizes the probe, you can continue probe configuration and administration using the Probes Tab. Use the following procedure to configure probe settings and physical device ports.

Refer to Iris Configuration and Administration Workflow for more information on the tasks you perform for configuring and maintaining the Iris system.

To Configure G10 Probe Settings

When the probe is first configured and you view it in the Probes tab, the assigned Probe ID appears as the probe name. This ID and name are seen in other applications as well as in alarms.

1. Click the Probes Tab.
2. In the Probes List, select a G10 probe to display its settings in the Probe Details Tab. Probes that have lost communication to the Iris server are shown in gray text.
3. In the Probe Details tab, modify the Probe Name and Probe Description.
4. Select the store to disk configuration for the probe. See Managing Iris Data Storage for details about store to disk profiles.

To Configure Physical Device Ports

To establish link traffic direction, you must configure ports and link capacity for each link physically connected to the G10 probe. If this has already been configured by the system installer, you can make necessary modifications. Defining Physical Device ports ensures the accurate flow of traffic data into the Iris server.

1. Click the Probes Tab.
2. In the Probes List, select a G10 probe from the list of available probes. Settings for the probe appear in the Probe Details Area and the Physical Device Ports Area.
3. In the Direction column for each port, select **RX**, **TX**, or **Span** (by default, all ports have an RX direction). These settings depend on whether the monitored network physically connects to the G10 via span/mirror ports or optical tap/splitters. See Physical Device Port Configuration Examples for details.
   - **Optical Tap/Splitter Ports:**these connections can only monitor in one direction, so **RX** or **TX** are valid options.
   - **Span/Mirror Ports:**these connections can monitor in any direction, so **RX**, **TX**, or **Span** are valid options.
4. Disable unused ports for the selected probe by clicking their corresponding cell in the **Enabled** column to clear the checkmark. By default, all ports are enabled or have a value of "true."
5. To disable light transmission for ports configured for an optical tap/splitter, click the corresponding cell in the **TX Enabled** column to clear the checkmark. By default, all ports are enabled or have a value of "true."
6. **1G Ports Only**: Set this field based on whether the 1G port is physically configured to support span ports or tap ports.
   - **1G Span Ports:** Op Mode=Negotiate; select Full Duplex or Half Duplex only if the monitored equipment is not configured to auto-negotiate.
   - **1G Tap Ports:** Op Mode=Full Duplex is recommended for most configurations; Half Duplex may be required in certain configurations.

Op Mode is disabled for 10G ports; the Iris system supports only the default Negotiate setting.

7. To save the G10 probe settings, click **Save**.

If you are modifying the Direction on an existing link, the probe must be restarted for changes to take effect. Contact Customer Support for details. If you are initially configuring the port, a restart is not necessary. A system restart can take up to 15 minutes.

To Customize G10 Probe Timing per Probe

You can configure the G10 probe for NTP timing or IRIG timing. Refer to G10 Probe Timing for details about the different options.

Probes require minimum software version 13.1 to support IRIG timing. See G10 Probe Timing for details and hardware requirements.

1. NTP servers must be defined in the Servers tab before you can customize timing settings per probe. See Defining Servers for details.
2. Click the Probes Tab.
3. In the Probes List, select a G10 probe from the list of available probes. Settings for the probe appear in the Probe Details Area.
4. Click the Timing Control tab.
5. Configure NTP Server settings and IRIG setting per probe. Refer to G10 Probe Timing for details.
6. To save the G10 probe timing settings, click **Save**.

Configuring GeoSoft RAN Probes

Probes are installed and configured at the installation site so that they can communicate with the Iris server. Once the Iris server recognizes the probe, you can continue probe configuration and administration using the Probes Tab.

GeoSoft RAN probes are the TekComms' implementation of the Trace Collection Entity (TCE) specification as defined by 3GPP TS 32.421, 32.422 and 32.423. TCE describes a soft probe way of network monitoring currently focused on RNC and eNodeB Trace Ports which provides Uu (Iub), S1/Iu and X2 (Iur) Signaling data.

When the probe is first configured and you view it in the Iris Probes Tab, the assigned Probe ID appears as the probe name. This ID and name are seen in other applications as well as in alarms. To configure the GeoSoft RAN settings, proceed as follows:

1. Click the Probes Tab and select a GeoSoft RAN probe in the Probe List. The Probe Details Tab displays the settings of the selected probe. Probes that have lost communication to the Iris server are shown in gray text.
2. In the Probe Details Tab, modify the Probe Name and Probe Description.
3. Open the gSoft Configuration Tab. Here you can customize the MME or RNC Nodes to be monitored by the GeoSoft RAN probe and configure the eNodeB Trace Port application.
4. In the Monitored MME / RNC Nodes area of the gSoft Configuration Tab, open the list of Monitored MME/RNC Nodes by pressing the ... button. By pressing this button, the **Select monitored MME/RNC Nodes** dialog box opens. Select the MME/RNC nodes to be monitored by the GeoSoft probe and confirm your settings by pressing OK (as described in the appropriate section of the gSoft Configuration Tab topic).
5. In the Trace Port Configuration area of the gSoft Configuration Tab, enter the probe and server settings for the trace ports to be monitored. In this area, each line represents one TCE data feed.

   Configure up to five different TCE data feeds per probe. Start this configuration by pressing the **Add File Mode** or **Add Stream Mode button**:

   - Press the **Add File Mode** button to configure a file based data feed. File based data feeds are feeds of TCE data that are provided as zip files for download.

     After pressing the **Add File Mode** button, the **File Mode** dialog box opens. Configure the data feed settings such as technology, vendor information, and server credentials in the **File Mode** dialog box as described in the appropriate section of the gSoft Configuration Tab topic.

   - Press the **Add Stream Mode** button to configure a stream based data feed. Stream based data feeds are feeds of TCE data that are provided by a TCP stream.

     After pressing the **Add Stream Mode** button, the **Stream Mode** dialog box opens. Configure the data feed settings, such as technology, vendor information, and server credentials in the **Stream Mode** dialog box as described in the appropriate section of the gSoft Configuration Tab topic.
6. Before starting your measurements, ensure that the configuration settings on the vendor side correspond to your GeoSoft RAN settings.

NOTE: For 3G GeoSoft RAN probes, you can configure an additional RAN Intelligence Feed for geolocation analyses. This enhanced xDR feed includes RAN statistics and measurement reports. For RIF configuration refer to the RIF Profile Tab topic.

Refer to Iris Configuration and Administration Workflow for more information on the tasks you perform for configuring and maintaining the Iris system.

G10 Probe Timing

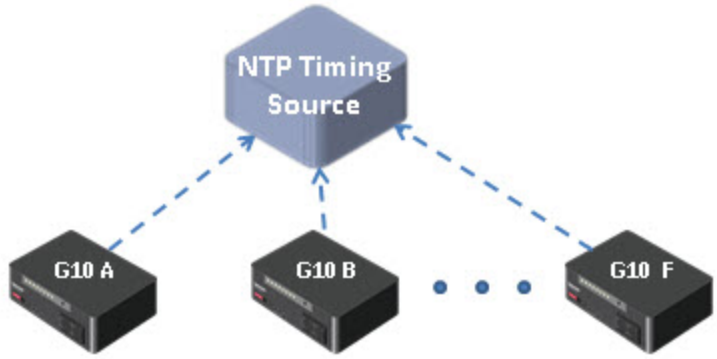
The G10 Probe supports NTP and IRIG timing in the following scenarios.

- NTP Timing from Defined NTP Servers
- IRIG Timing from Master G10
- IRIG Timing from Third-Party Source

NTP Timing from Defined NTP Servers

G10 probes support multiple NTP server references which provide increased timing reliability, especially in cases of failure of the primary NTP server reference. Multiple timing servers also allow server maintenance without the need to manually reconfigure the G10 probes.

- G10 probes select the best available NTP server from the list and use it as their timing reference.
- When maintenance is required on the server acting as the active NTP reference, the G10 probe automatically selects another server in the list without user intervention.



OAM Configuration	On the Servers tab, define the IP addresses of servers you want to use as NTP timing sources. ***Tektronix Communications recommends provisioning three or more servers as a best practice for reliability of timing references.*** On the Timing Control Tab per probe, the IRIG setting is disabled. • NTP Servers: default or custom • IRIG Status: Disabled
Hardware Configuration	• All G10s connect to NTP timing sources over LAN • IIC RTM SYS CLK jumper settings are not applicable in this scenario

IRIG Timing from Master G10

Probes require minimum software version 13.1 to support IRIG timing.

G10s support IRIG timing references to and between probes allowing for greater monitoring accuracy at facilities with multiple probes. Support for the IRIG timing interface allows G10 probes to share timing with other G10 probes and with 14U and 2U GeoProbes. A G10 probe can operate as an IRIG master or an IRIG slave.

The G10 designated as the IRIG timing master to other probes must have a valid timing reference such as NTP. The IRIG slaves use IRIG timing reference from the IRIG master G10; however, the slave G10s also require NTP timing reference for the time of day.

OAM Configuration	On the Timing Control Tab per probe, configure following settings for each G10: **IRIG Master A** • NTP Servers: default or custom • IRIG Status: Master **IRIG Slaves (B, C, D, E, F)** • NTP Servers: default • IRIG Status: Slave • IRIG Master: G10 A
Hardware Configuration	• Master G10 connects to NTP timing source over LAN • Slave G10s connect directly to Master G10 or to each other • Master G10 A and Slave G10 F: set IIC RTM SYSCLK jumper settings to TERMINATED • Slave G10 B, C, D, E: set IIC RTM SYSCLK jumper settings to BRIDGED • Cable the G10s at SYSCLK ports using SYSCLK cables to form a daisy-chain from probe to probe. Refer to the G10 hardware documentation for details about SYS CLK jumper settings.

IRIG Timing from Third-Party Source

Probes require minimum software version 13.1 to support IRIG timing.

G10 probes support receiving IRIG timing from a third-party source, such as GPS.

OAM Configuration	On the Timing Control Tab per probe, configure following settings for each G10: • NTP Servers: default or custom • IRIG Status: Slave • IRIG Master: Enter a name to identify the GPS Timing Source (such as "ExternalGPS"). Spaces are not allowed.

Hardware Configuration	• Slave G10s connect directly to GPS timing source and to each other.
	• GPS Source and G10 F: set to TERMINATED.
	  • For G10 F, set IIC RTM SYS CLK jumper settings to TERMINATED.
	  • For GPS timing source, refer to the product's documentation for configuring the IRIG output for that unit. You must also configure an NTP timing source for time of day reference.
	• Slave G10 A, B, C, D, E: set IIC RTM SYS CLK jumper settings to BRIDGED.
	Refer to the G10 hardware documentation for details about SYS CLK jumper settings.

Probes Supported by Iris

With the introduction of the GeoProbe G10, Tektronix maintains the commitment to supporting interoperability with existing GeoProbe SpIprobe deployments. As the framework behind the Network Intelligence portfolio, IrisView provides a seamless user experience for targeted Iris applications within the framework, regardless of the underlying GeoProbe data source. The Iris solution supports the following probes.

Application	GeoProbe Compatibility	Launched From ...
ITA	G10	IrisView
ISA	G10, 14U, 3U, 2U, 12U, GeoSoft	
IPI	G10, 14U, 3U, 2U, 12U	
Iris Network Maps	G10, 14U, 3U, 2U, 12U	
ACE	G10, 14U, 3U, 2U, 12U	
PA	G10, 14U, 3U, 2U,	
	14U, 3U, 2U	SpImain
		GeoProbe Network Maps

ISA, PA, and IPI applications require access to historical data stored on G10 probe storage arrays.
The Automated Controller Engine (ACE) application requires deployment of at least one DirectQuality PowerProbe in order to run Active Tests for the Iris solution.

GeoProbe Family

The GeoProbe family of probes includes 2U, 12U, and 14U SpIprobes and G10 Probes.

14U, 3U, 2U, and 12U SpIprobes

Only G10 probes are administered within the IrisView Admin Probes tab. SpIprobes are administered using the GeoProbe software. Refer to the GeoProbe product documentation for information regarding SpIprobes.

The 14U, 3U, 2U, and 12U SpIprobes monitor fixed, mobile, and converged networks and are industry-standard probes, correlating data across multi-protocol networks. Collectively, these probes are referred to as SpIprobes. Refer to the GeoProbe product documentation for more details about these probes.

G10 Probes

The following table describes the different GeoProbe G10 configuration options:

G10 Configuration	Supported HW	Configuration Details
8 x 1G	IIC100 + SRM100RTM IAP100 + PRM100 RTM IAP200 + PRM200 RTM IAP320 + PRM300RTM	Single chassis probe configuration • Supports 8 physical 1G connections • Can be upgraded in the field to a Mixed Model

G10 Configuration	Supported HW	Configuration Details

Mixed Model (1G and 10G)	IIC100 + TRM100 RTM
	IIC200 + SRM200 RTM
	IIC200 + TRM100 RTM*
	IAP100 + PRM100 RTM
	IAP200 + PRM200 RTM
	IAP320 + PRM300RTM
		Single chassis probe configuration
		• Provides support for both 1G and 10G Ethernet connections on one probe.
		• Various combinations are supported with the following maximums:
		  • Maximum support of 8 total ports (1G + 10G)
		  • Maximum support of 4 10G ports
		*The IIC200 + TRM100 RTM configuration is only supported for standalone probe configurations monitoring eHRPD.

Media Probe	IIC100 + TRM100 RTM**
	IIC200 + SRM200 RTM
	IAP100 + PRM100 RTM
	IAP200 + PRM200 RTM
	IAP320 + PRM300RTM
		Two-chassis probe configuration for supporting RTP media monitoring
		• Primary Chassis supports:
		  • Maximum of 8 total ports (1G + 10G)
		  • Maximum of 4 10G ports
		• Expansion Chassis provides additional data processing support
		**Due to the Media probe and probe configuration, deployments with IIC100/TRM100 RTM have a maximum of TWO 10G physical ports available to monitor traffic.

Control Plane Probe	IIC100 + TRM100 RTM**
	IIC200 + SRM200 RTM
	IAP100 + PRM100 RTM
	IAP200 + PRM200 RTM
	IAP320 + PRM300RTM
		Two-chassis probe configuration for supporting Mobility Management Entity (MME) monitoring
		• Primary Chassis supports:
		  • Maximum of 8 total ports (1G + 10G)
		  • Maximum of 4 10G ports
		• Expansion Chassis provides additional data processing support
		**Due to the Control Plane probe configuration, deployments with IIC100/TRM100 RTM have a maximum of TWO 10G physical ports available to monitor traffic.
		***The control plane probe only supports the IIC100/IAP200 configuration; the IIC100/IAP320 configuration is not supported.

Refer to Configuring Probes for details about configuring physical device ports and probe settings. Refer to the ***G10 Hardware Maintenance Guide*** for more information about the G10 Probe.

PowerProbes

As part of the Active Assurance product line, the PowerProbe active test probes are designed for advanced Quality of Experience (QoE) testing over PSTN and next-generation networks. With a broad range of interfaces supporting all standard signaling protocols, the PowerProbes support a growing library of over 40 test agents to cover evolving service quality testing needs.

Remotely managed and highly secure, the PowerProbes enable scalable end-to-end, bi-directional voice, fax, video, and IP tests that measure over 300 user-perceived service quality metrics using an array of standards-based and patented algorithms. Controlled by Tektronix' DirectQuality active test automation OSS, the PowerProbes perform on-demand and scheduled tests for proactive service monitoring, SLA validation, carrier benchmarking, and troubleshooting applications.

PowerProbes are administered using the DirectQuality software. Refer to the DirectQuality documentation for information regarding PowerProbes.

GeoSoft RAN Probes

GeoSoft RAN probes are soft probes, acting as mediation device interfacing with the OMC and eNB elements. The GeoSoft RAN probe mediates the RAN data to the Iris applications suite and NSA/Optimon systems.

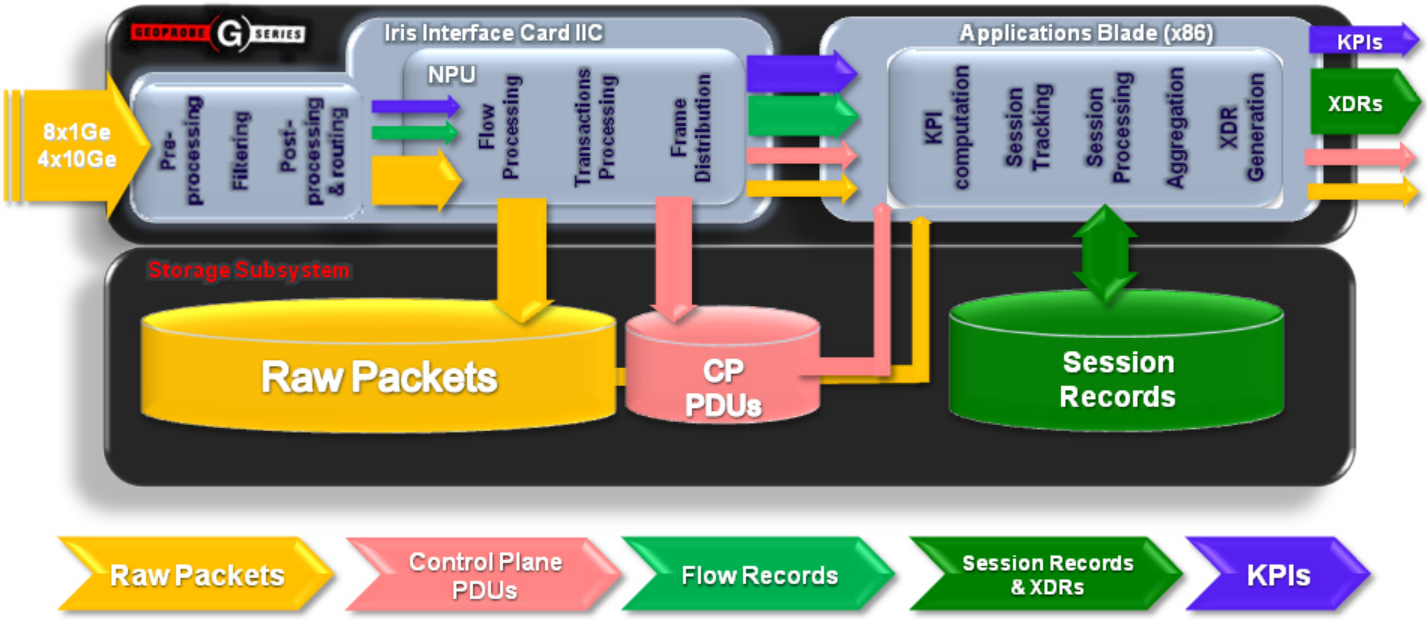
Refer to Probes Tab and gSoft Configuration Tab for details about configuring GeoSoft RAN probes.

G10 Data Processing Overview

GeoProbe G10 connects to the monitored network via a physical interface at the link port. Raw packets are processed in real-time as they reach the Iris Interface Card (line rate processing functions) and forwarded (stream to disk functions) to the Storage Subsystem.

In parallel, the Iris Interface Card sends control plane traffic to the Application Blade for correlation, xDR generation and KPI aggregation (control plane processing functions).

Once processed, resulting xDRs, KPIs, and processed packets are made available for use by the various Iris Network Management applications.



Iris Data Types

The following table defines each data type, the Iris applications that utilize it, and the type of storage used. As a default, control plane data supported in ISA is stored in long-term volumes. See Managing Iris Data Storage for more information.

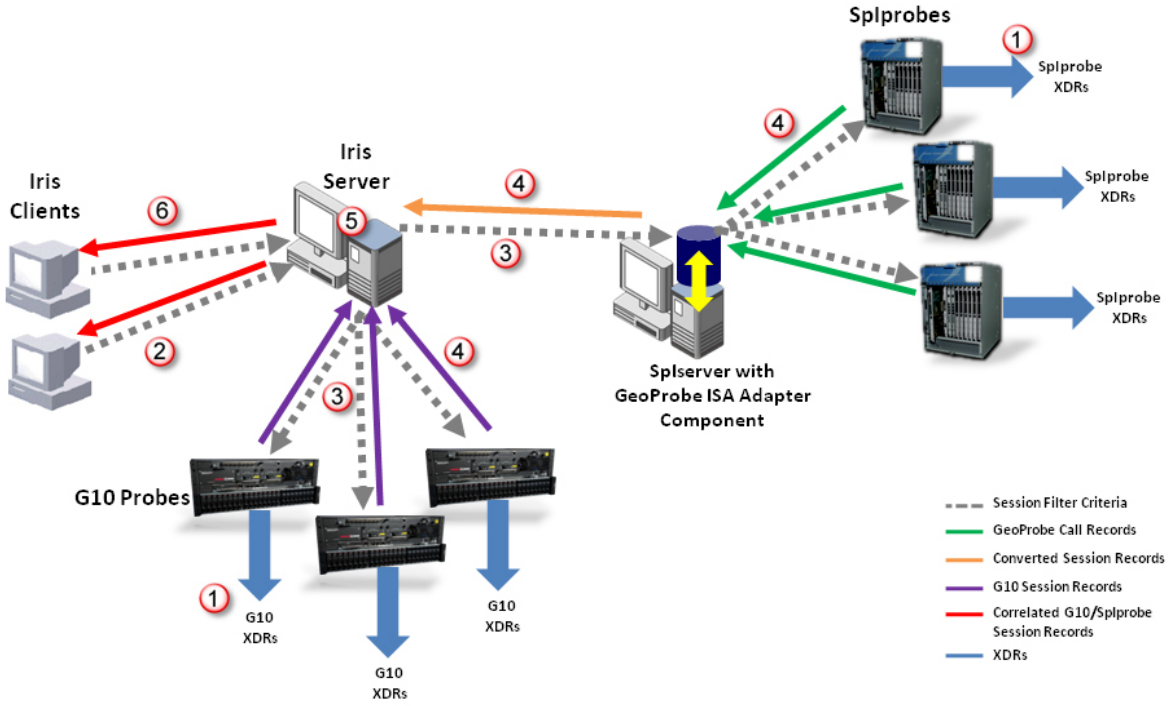
Data Output Formats	Iris Data Storage	Iris Application Use					
		PA	ITA	ISA	Policy Engine (Alarms)	IPI	ACE
Raw Packets • Raw data that is pre-processed (time-stamping, filtering, classification and routing) by IIC	Short-term volume on Storage Array (S2D)	X		X			
Control Plane PDUs • Control plane packets (such as GTP-C, Radius, RTSP, and DNS)	Long-term volume on Storage Array (S2D)	X		X			
Flow Records • Summaries of User Plane data (such as HTTP and Email) • Do not contain PDUs • Internal to probe for KPI processing and aggregation; not stored or forwarded to applications	Not applicable		X	X			
Session Records • Complete summaries of calls or transactions • Contain all control plane PDUs • Contain aggregated flow record summaries for user plane traffic • Exclusively used for ISA; not forwarded to receivers	Long-term volume on Storage Array (SR2D)			X			

Data Output Formats	Iris Data Storage	Iris Application Use					
		PA	ITA	ISA	Policy Engine (Alarms)	IPI	ACE
XDRs • Complete summaries of calls or transactions created at the close of the call/transaction • Contain session summaries with correlated flow record summaries • Do not contain PDUs • Contain extracted Information Elements (IEs) from PDUs used for KPI calculations • Forwarded to DataCast	Not applicable					X	X
KPIs • Key Performance Indicators (KPIs) used to measure quality of performance of network activity • Calculated from Raw Packets, Flow Records, or XDRs	Database on Server		X		X	X	X

Iris Network Data Flow

ISA Data Flow

All ISA trace functions are supported across deployed G10 and SpIprobe hardware for a comprehensive and correlated end-to-end view. Customers who have ISA and whose deployment includes SpIprobes will require a GeoProbe ISA Adapter component on the SpIserver. This component provides ISA communications to the SpIserver. Refer to Defining Servers for information about configuring IrisView to support the Adapter Server.



1	**Probes collect data, correlate sessions, and process XDRs in real time, 24 hours a day, 7 days a week.** • Probes forward XDRs to DataCast • Control Plane and User Plane PDUs are stored to disk (S2D) • Session Records are stored to disk (SR2D) or retained in memory (for active calls)
2	**When user initiates ISA session, the Iris Clients send session filter criteria to Iris Server.**

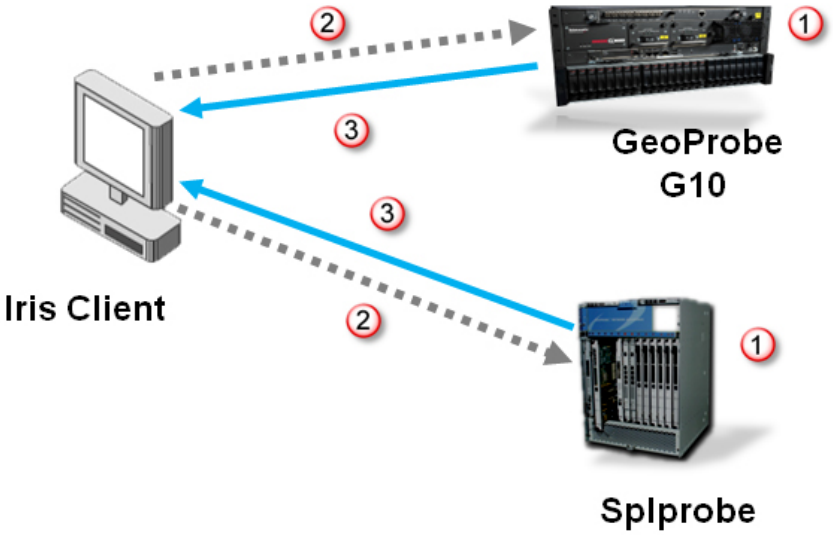
3	**Iris Server communicates session filter criteria.**
	• to G10s
	• to ISA Adapter
	  • Queries SpIserver for topology and configuration information to identify SpIprobes monitoring selected nodes
	  • Forwards session filter criteria information to those SpIprobes, and requests call records matching session filter criteria

4	**Probes forward Call/Session Records.**
	• **G10s** forward session records and flow record summaries to Iris server
	• **SpIprobes** forward call records to ISA Adapter
	  • Converts call records to ISA session records
	  • Forwards session records to Iris server

5	**Iris server performs a quick correlation of G10 and SpIprobe session records into multi-protocol (MPC) and multi-probe session records.** • Based on merged data and MPC rules and algorithms, additional MPC searches could result in more call leg records being retrieved from probes and merged into MPC session records
6	**Iris server forwards correlated session records and flow record summaries to Iris Client.** • Users view session record results matching their filter criteria in ISA GUI • Users can expand flow record summaries to view associated user plane PDUs

PA Data Flow

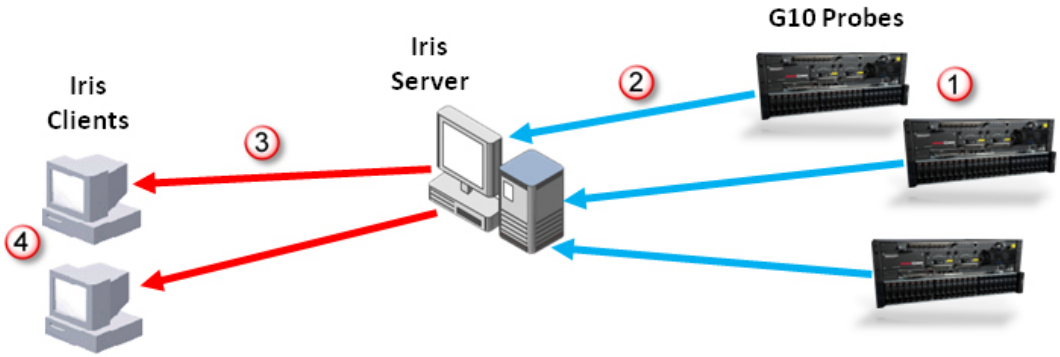
The PA application allows you to select the specific probe from which you want to capture packet data. PA supports 2U, 3U, and 14U SpIprobes and G10 probes. Once you select the links to monitor on the IrisView client, a capture session between the client and applicable Probes is established.



1	**Probes collect PDUs.** • Probes forward Streamer PDUs to storage arrays (S2D)
2	**When user initiates PA session, the Iris Clients send capture filter criteria to probes.** • Probes store PDUs in their capture session buffers
3	**Probes forward PDUs matching filter criteria to Client for viewing and analysis.** • Users can apply search and display filters • Users can save and export data

ITA Data Flow

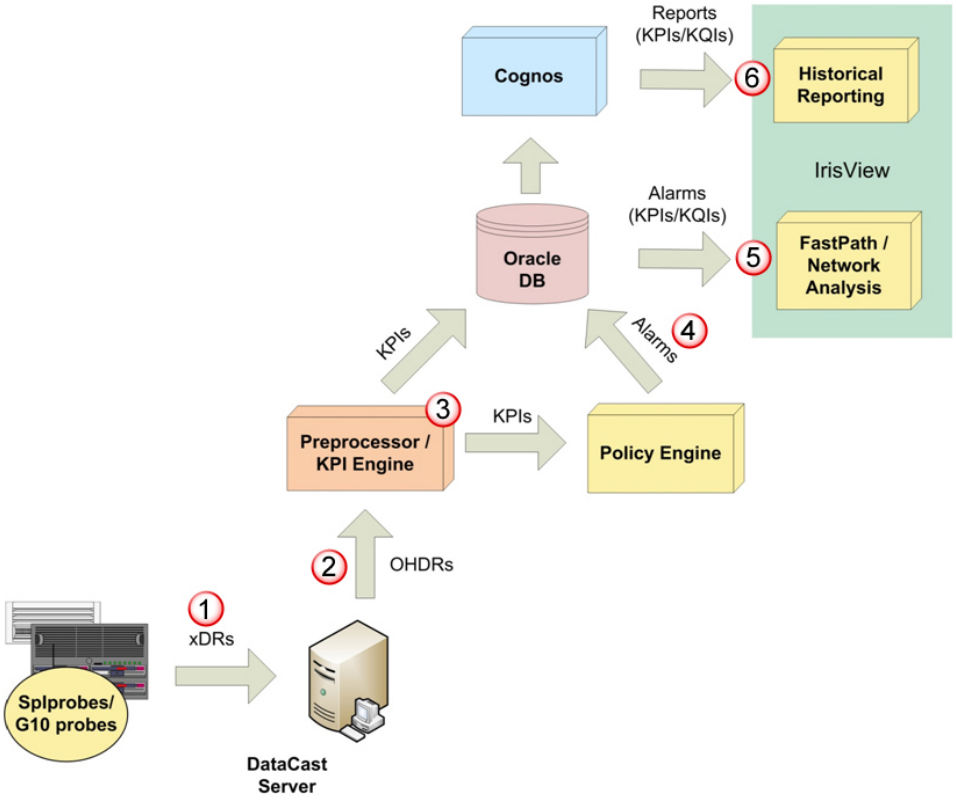
ITA provides an end-to-end view of network traffic, protocol types, and application and host bandwidth usage for all network data monitored by G10 probes. ITA does not support SpIprobes.



1	**G10s collect data for all supported links, VLANs, nodes, node groups, and application protocols.** • G10s process user plane and control plane PDUs into flow records and KPIs
2	**G10s forward KPIs to Iris server (updated with new data every minute).** • Iris server calculates, aggregates, and stores KPIs in the database
3	**Iris server forwards KPI information to client when users launch ITA session.**
4	**Users access Links, Applications, Nodes, and Node Groups landing pages and drill down to different dashlets to analyze data.**

IPI Data Flow

The majority of data processing for the IPI application occurs after Programmable Data Records (XDRs) are forwarded to the DataCast server from SPIprobes and G10 probes.



1	**Probes collect data and process Programmable Data Records (XDRs) in real time, 24 hours a day, 7 days a week.** • Probes forward XDRs to DataCast server.
2	**DataCast processes XDRs into Output Hybrid Data Records (OHDRs) and forwards them to the IPI Preprocessor and KPI Engine.**
3	**IPI Preprocessor and KPI Engine calculate and aggregate KPIs.** • KPI Engine forwards KPIs to Policy Engine for use in alarm policies • KPI Engine stores KPIs in Oracle Database. (An IPI database schema is available upon request; contact Tektronix Customer Support for more information.) • IPI Preprocessor and KPI Engine forward failed OHDRs to Oracle Database • Tektronix can also configure KPIs to be exported to third party vendors; contact Customer Support for details.
4	**Policy Engine generates alarms based on defined alarm policies.** • Administrator configures alarm policies by defining thresholds for combinations of KPIs and KQIs • When KPI thresholds are breached, the Policy Engine forwards alarms to the Oracle database
5	**Users access FastPath and Proactive Network Analysis using different dashlets to analyze data.**
6	**Users access Historical Reporting tool to analyze trends in data.**

Iris Data Storage

All GeoProbe G10 systems support a dual controller disk array to provide disk space for applications requiring extensive data storage. Each storage enclosure holds up to 24 SAS disk drives.

The storage subsystem consists of the controller and expansion enclosures. Iris supports two controller enclosures, and each controller enclosure supports three expansion enclosures for a total of eight. Refer to the ***G10 Hardware Maintenance Guide*** for more information about the Iris storage array hardware.

Storage Methods

In order to support non-real time traffic monitoring applications (that is, near-real-time or historical analysis applications) the G10 probe manages data storage using the following methods:

- Store-to-Disk (S2D) stores only packet data to short-term or long-term S2D volumes on the storage array. As a default, control plane protocol data supported in ISA is stored in long-term volumes. User plane protocol data and control plane data not supported in ISA is stored in short-term volumes. The Iris administrator can configure where data is stored using the Managing Store to Disk Options in the Store to Disk Tab.
- Session Records to Disk (SR2D) stores session records and all of the indexes required for searching for them. The Iris system creates session records for every control plane protocol and stores them in a long-term SR2D volume separate from the S2D volumes.

Refer to Storage Array Configuration for details about storage array configuration profiles.

IP Packet Truncation

In order to increase efficiency of data processing and storage, the Iris system supports truncating the user payload carried in IP user plane packets. The following table describes G10 packet truncation support.

You can configure which protocols you want to truncate in the Store to Disk Tab. Refer to Managing Iris Data Storage for details.

G10 Truncates:	G10 DOES NOT Truncate:

• IP user plane packets, starting with the first byte of the packet
• Any Layer 7 protocol (such as HTTP and GTP)
• HTTP packets - HTTP truncation can only be enabled or disabled in the Store to Disk tab; you cannot control the amount of HTTP payload that is truncated. The G10 truncates HTTP packets as follows:
  • Truncation occurs in the Flow NPU as the packet is written to disk.
  • If the beginning of the message headers is present and the message body is present, then the packet is truncated at the beginning of the message body.
  • If the beginning of the message headers is present and the message body is not present, then the packet is not truncated.
  • If the beginning of the message headers is not present, then the packet is truncated at the end of the TCP header.
  • Pipelining HTTP/TCP segments are truncated at the end of the last header.
• Tunneled IP, TCP, UDP packets (over GTP)
  • The packet is truncated after GTP header
  • If the configured truncation length is less than the layer2, tunnel layer3, tunnel layer4, layer3, and layer4 header lengths, then the packet will be truncated at the end of the last header.
	• Control Plane packets
	• Layer 2 through Layer 4 protocols (such as IP, TCP and UDP)
	• IP fragments
	• Reassembled IP datagrams

Storage Array Configuration

Tektronix engineers analyze the customer's data storage requirements and configure disk arrays connected to the G10 probes by selecting the appropriate profile based on storage requirements.

Data is stored in one of the following archives:

- S2D Long-Term (LT) packet data
- S2D Short-Term (ST) packet data
- S2D Decrypted (DC) packet data
- SR2D session record data and associated indexes

Refer to Iris Data Storage for more information about storage arrays and storage methods. See Iris Data Types for details about the type of data storage used per Iris application.

Do not change the Storage Maintenance settings, as this can result in loss of data or system configuration.

TD140 Architecture Overview

The TD140 Traffic Distributor is a GTPv1/GTPv2 load balancing network element used as a Gn/LTE monitoring solution to distribute coherent GTP sessions from the S1-U, S11, S5/S8, S4, and Gn interfaces among a pool of G10 probes. This

product provides a complete, independent solution with software and hardware integrated into a common environment.

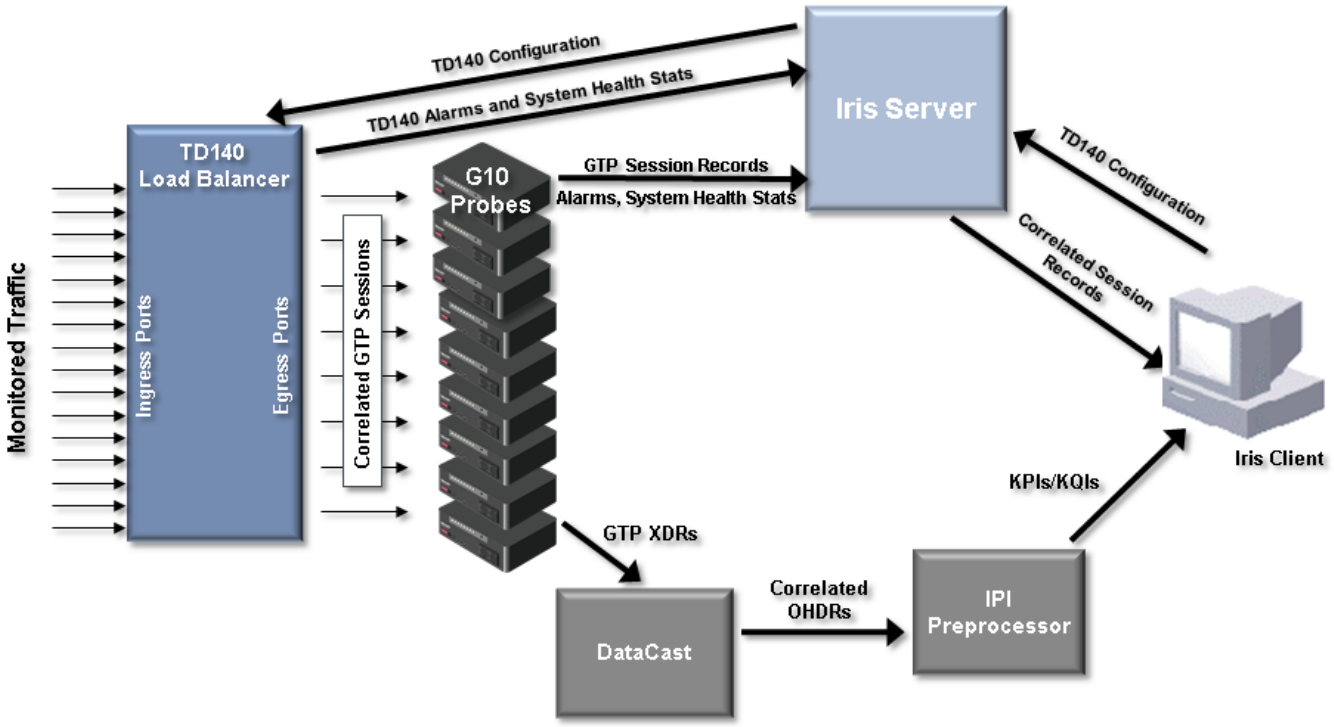
The TD140 supports all standalone G10 hardware configurations; up to 16 G10 probes are supported per TD140.

See the following sections for details about the TD140:

- TD140 Configuration Workflow
- Upgrading TD140 Software

TD140 Architecture Overview

The following diagram illustrates the TD140 architecture and data flow.



Element	Function
TD140	• At ingress ports, TD140 collects GTP traffic from S1-U, S11, S5/S8, S4, and Gn interfaces in the packet core network. • Other traffic (non-GTPv1/v2 IP protocols) is load balanced based on IP • At egress ports, TD140 distributes packets based on session correlation among a pool of G10s. It adds metadata including timestamp and port tag. • Generates alarms and forwards to Iris server. • Generates system health statistics for future use.
G10 Probes	• Generates GTP session records and forwards to the Iris server. • Generates GTP XDRs and streams them to DataCast. • Generates alarms and forwards to Iris server. • Generates system health statistics for future use.
Iris Server	• Correlates session records and forwards to ISA. Stores TD140 configuration settings (configured in Irisview Admin on Iris client)

DataCast	• Correlates XDRs and processes them into Output Hybrid Data Records (OHDRs) and forwards them to the IPI preprocessor.
IPI Preprocessor	• Processes OHDRs and calculates and aggregates KPIs for use in IPI applications.
Iris Client	• Admins configure TD140 settings. • Users view correlated session record results matching their filter criteria in ISA. • Users view KPIs/KQIs in IPI applications and reports.

TD140 Configuration Workflow

Once the TD140 is physically installed, the system installer configures the TD140 with the IP address it needs to establish communications with the Iris Server for configuration and maintenance.

After the TD140 connects to the IrisView server, you can view it the Probes tab. All G10 probes and TD140s appear in the Probe Tab.

To Configure TD140 Devices

For first time setup, it is recommended you follow these steps to ensure optimum provisioning of the TD140.

1. Bind the G10 probe to the TD140 Device.
   To Bind a G10 Probe to a TD140

To Bind a G10 to a TD140

   a. On the Probes tab, select a G10 probe in the Probe List pane.

   b. Click the Bind to TD140 Device button in the Probe Details tab. This button is only visible if at least one TD140 device has connected to the Iris server. A message appears warning you of the following consequences:

      - Any currently configured physical links on the G10 probe will be deleted
      - Loss of data will occur on G10 probe and TD140.
      - Once binding starts, the changes cannot be reverted.

   c. From the selection dialog box, perform the following:

      - Select the TD140 to associate with the G10.
      - Select the traffic type the G10 will be handling.

   d. Click **OK**. The G10 will be moved under the TD140 device in the Probe List pane.

2. Define TD140 Ingress and Egress Port settings in the TD140 Ports tab.
3. Define TD140 device parameters in the TD140 Details tab.
4. Configure traffic and session details for associated G10s in the Managed Probes tab.
5. Map the TD140 physical device ingress ports to links in the Physical Links Details pane. When you select a TD140 device, the ingress ports appear in the Physical Device Ports area.
6. Configure the G10 probes connecting to the TD140 egress ports.
   - Set the following physical device port settings on the Probe Details pane.
     - Set **Enabled** column to **True** for all 10G ports that are physically connected to TD140; set **Enabled** column to **False** for all 10G ports not connected to the TD140.

- Set **Op Mode** to Negotiate for enabled 10G ports
- The Direction setting (TX, RX, Span) is ignored by the G10 probe when it is connected to a TD140.

Chapter 4 Topology Management

Monitored network topology is the core of any monitoring solution. The Topology Management feature ensures that network operators can manage the provisioning of all network entities (physical links, logical links, protocols, domains, and nodes) to enable continuous monitoring.

In the Topology Management tab, you can define characteristics for each entity, and add entities to specific groups to enhance logical monitoring capabilities for network operators in various geographic locations.

The Managed Objects tab on the Topology Management Tab enables you to perform the following tasks:

- Configuring Applications
- Configuring Domains
- Configuring Logical Links
- Configuring Nodes
- Configuring Physical Links
- Creating and Managing Entity Groups
- Configuring Traffic Classification
- Enabling ISUP H248/MGCP Correlation for ISA

Refer to the following sections for additional information:

- Generic-OnDemand Nodes
- Topology Auto-Detection
- Iris Application Support of Configured Entities

Configuring Physical Links

Iris' Physical Links feature on the Topology Tab enables you to map your physical device ports to links. These links can be used for filtering and viewing data per link or link group within Iris applications.

For IP monitoring, you can also assign nodes to physical links to be used when viewing IP packet flow in the ISA Ladder diagram (with "Show on Physical Link" view).

Prerequisites

- You must configure Physical Device Ports on the Probes tab to be able to assign to links. Refer to Configuring Probes for details.
- If you want to assign nodes as endpoints to a physical link, the nodes must exist in the Iris system in order for you to assign them to the physical link. See the Node Details Pane and Configuring Nodes for details about configuring nodes for the Iris system.

To Assign Physical Device Ports

1. Click the Topology tab to display the Managed Objects Tab.
2. Select **Physical Links** in the Filter Entity Type drop-down list.
3. Click **Add Entity**. The Physical Link Details Pane appears showing the Link Details Tab with blank entry fields.
4. Enter a name for the link. Remember that this name is viewed in Iris applications, so be consistent with link naming schemes and be descriptive of the probe that the link is mapped to.

5. Select a Probe from the drop-down list. The configured physical device ports for that probe display in the Physical Link Details.
6. Select one or more physical device ports to assign to the current link.
7. Click **Save**. Links are downloaded to the probe and it starts monitoring traffic for the defined physical devices.
8. To add the link to an existing physical link group, click **Add to Group**. See Configuring Entity Groups for details about creating new entity groups.
    a. Select the name of a link group from the drop-down menu.
    b. Click **OK** to save the changes and close the dialog box.

To Assign Nodes for ISA Ladder Diagram Display

Assigning nodes to physical links is only used for viewing IP data flows in the ISA ladder diagram (with the "Show Physical Link" option enabled). See the Physical Link Details pane for details.

1. Select the **Node Details** tab on the Physical Link Details pane.
2. To assign Node information for a physical link perform the following (see the Physical Link Details pane for more details):
    - If you **know the endpoints** of the physical link, define an RX (destination) node and TX (source) node for the link by clicking the **RX Node** or **TX Node** field (or the **...** button) to open the Select a Node dialog box.
    - If you **do not know one or both endpoints** or you do not want to use nodes configured in the Iris system, click the **Auto-generate nodes** option to enable it. Iris auto-generates endpoints for the link for any undefined RX or TX node. RX (destination) node name format is "LinkName_DL"; TX (source) node name format is "LinkName_UL".
3. Click **Save**. Links are downloaded to the probe and it starts monitoring traffic for the defined physical devices.

Configuring Nodes

The Node Details pane enables you to view configuration details for all nodes defined in the Iris system by manual configuration, bulk import, or auto-detection. Use the procedures in this section if you want to create or modify an individual node; if you want to manage multiple nodes at once, refer to Using CSV Import/Export.

To Configure a Node

1. Click the Topology Tab. The Managed Objects Tab shows by default all monitored nodes.
2. Perform one of the following actions:
    - Click **Add Entity**. The Node Details Pane displays with blank entry fields.
    - Select the checkbox corresponding to the node you want to modify. The Entity Details Pane displays with the selected node's information.
3. Enter a name or update the existing node name. Remember that this name is viewed in Iris applications, so be consistent with node naming schemes and be descriptive.
4. Select the **ITA Enabled** check box to enable or disable the node to collect data for the ITA application.

    By default, most node types are enabled for the ITA application. You can enable nodes as needed; however, you can only enable Generic-OnDemand Nodes through the scheduling feature (see the Node Details pane for scheduling details).
5. Select the node type from the drop-down list. A Point Codes tab appears for select node types that support point code configuration.

Node types are assigned default protocols..

6. Define IP addresses or point codes for the node. IP addresses are optional for nodes using the Transparent Network Device node type; see the Node Details pane for details.
    - **IP addresses:** Enter or modify the IP address in IPv4 or IPv6 format. See Supported IP Address Formats and Syntax for details. An error message appears if the IP address you enter conflicts with an IP address of an existing node.
    - **Point Codes:** The Point Codes tab is only accessible for select node types; see Node Details for configuration details.
7. For Generic-OnDemand Nodes, define a schedule for activating this node. See Node Details for scheduling details.
8. Click **Save**. Node data is sent to the probes which start to collect transactional data for the selected protocols.
9. To add the node to an existing node group, click **Add to Group**. See Configuring Entity Groups for details about creating new entity groups.
    a. Select the name of a node group from the drop-down menu.
    b. Click **OK** to save the changes and close the dialog box.

Active/Standby Node Provisioning

Carriers are deploying network elements in an active/standby configuration to allow for failovers without the interruption of service for subscribers. Tektronix Communications' monitoring system provides visibility into the performance of each network element and clearly indicates the behavior of these network elements in failover cases. Redundant nodes have the following characteristics:

- One network element is active at any given time and the other network element is in standby mode
- Both elements use the **same** virtual IP address

Redundant nodes must be provisioned so Iris can differentiate between the active and standby nodes.

Node Provisioning

To monitor the node performance and the traffic change in a switchover scenario:

- Active and standby nodes must be monitored by different probes
    - Probes are assigned unique physical links
    - Physical link ID is used to differentiate the active and standby nodes
- Active and standby nodes are assigned Physical Link IDs in the Node Details pane. ***This feature does not apply to SIGTRAN nodes.***

The link between the active and standby network elements is NOT monitored by the probes. There is no session resiliency support on the monitoring system. In a case of failover, the sessions at the active probe are closed with timeout status and all new sessions are monitored at the initial standby node.

Node Provisioning Examples

Example 1: Invalid (Overlapping)

Two nodes with same IP range cannot be configured on the same probe.

NodeId	IP Range	Physical Link ID
1	1.1.1.1	1 (ProbeID=4098)
2	1.1.1.1	2 (ProbeID=4098)

Example 2: Invalid (Overlapping)

Two nodes with same IP range cannot be configured on the same probe. Because physical links are not configured for these nodes, it results in an error.

NodeId	IP Range	Physical Link ID
1	1.1.1.1	None
2	1.1.1.1	None

Example 3: Invalid (Overlapping)

Two nodes with same IP range cannot be configured if one of them has no physical link configured. The system will not allow the new node to be created until you specify a physical link for the existing node.

NodeId	IP Range	Physical Link ID
1	1.1.1.1	None
2	1.1.1.1	1 (ProbeID=4098)

Example 4: Valid (Non-overlapping)

Two nodes with same IP range are configured on different probes.

NodeId	IP Range	Physical Link ID
1	1.1.1.1	1 (ProbeID=4098)
2	1.1.1.1	11 (ProbeID=4099)

Example 5: Valid (Non-overlapping)

Two nodes with different IP ranges are configured on the same probe.

NodeId	IP Range	Physical Link ID
1	1.1.1.1	1 (ProbeID=4098)
2	2.2.2.2	1 (ProbeID=4098)

Generic-OnDemand Nodes

The Generic-OnDemand node type enables you to assign an individual IP address or a range of IP addresses to an individual node for ITA statistical tracking over a scheduled time period. Scheduling node activation enables users to target ITA statistics over a desired time frame (see Node Details for scheduling details).

You can configure a Generic-OnDemand node to support the following scenarios:

- Monitoring an individual HTTP server that is supporting smart phone usage during a major sporting event.
  - You configure a Generic-OnDemand node with the HTTP server's IP address (or range of IP addresses) and schedule activation for ITA monitoring for the duration of the sporting event.
  - Users monitor the node representing the HTTP server in ITA using the same workflows as with other nodes, filtering on the specific time period the node was scheduled as active.
- Monitoring a series of handsets introduced into the network to monitor their initial performance
  - You configure a Generic-OnDemand node with the mobile handsets' IP addresses (or range of IP addresses) and schedule activation for ITA monitoring for the initial launch.

- Users monitor the node representing the handsets in ITA using the same workflows as with other nodes, filtering on the specific time period the node was scheduled as active.

Refer to Iris Online Help for ITA workflow details.

Configuring Logical Links

The Logical Links pane enables you to view configuration details for all logical links defined in the Iris system by manual configuration or auto-detection. Use the procedures in this section if you want to create or modify a logical link.

Prerequisite

A logical link's associated nodes must exist with valid Node IDs (non-zero values) before you can add or modify logical links. Refer to Configuring Nodes for details.

To Configure a Logical Link

1. Click the **Topology Tab** to display the Managed Objects Tab.
2. Click **Logical Links** in the Filter Entity Type drop-down list.
3. Perform one of the following actions:
    a. Click **Add Entity**. The Logical Link Details Pane displays with blank entry fields.
    b. Select the checkbox corresponding to the logical link you want to modify. The Entity Details Pane displays with the selected link's information.
4. Enter the required Logical Link Details. *If a link has an incorrect endpoint defined, it must be deleted and recreated.*
5. Click the **Save** button. Logical link data is sent to the probes which start to collect data for the defined SCTP associations.

Configuring Entity Groups

After you configure entities, you can create logical groupings of these entities to enable precise group monitoring capabilities using the Iris applications. The current release only supports groups of physical links, nodes, or probes. See Entity Groups for more details.

To Create a Group

1. Click the Topology Tab. The Managed Objects Tab shows by default all monitored nodes.
2. Click the **Groups** tab. The Groups Pane displays the default group types: LinksGroupType, NodesGroupType, and ProbesGroupType. Any legacy groups are migrated into one of these group types.
3. Click the **New Group** button to open the Group dialog box.
4. Select a default Group Type from the drop-down menu: LinksGroupType, NodesGroupType, or ProbesGroupType.
5. Enter a name for the new group. Allowable characters include alphanumeric characters, minus (-), underscore (_), period (.), space ( ), colon (:), or slash (/).
6. Click **Save**. The new group is saved to the selected group type and appears in the Groups Pane.

To Add Entities to a Group (from the Groups Tab)

Follow these steps to add *physical links* or *nodes* to an existing group from the Groups tab. You can add *probes* to existing probe groups on the Probes Details Tab accessed from the Probes Tab.

Prerequisite

You must first create groups before you can add entities to them; for details, see To Create a Group.

1. Click the Groups tab.
2. Click **Add** on the Members Pane to open the Add Group Member(s) dialog box.
3. Select the entity type you want to add to a group. Only physical link groups, node groups, and probe groups are supported in the current release.
4. Select the group to which you will be adding entities. Group names display in the format [Group Entity] - [Group Name].
5. In the first column in the Managed Elements Pane, click the check boxes next to the entities you want to add to the entity group.
6. Click the **OK** button to save the selections and close the Add Group Member(s) Dialog Box. The window refreshes to display the group and its associated entities.

To Add Entities to a Group (from Managed Objects Tab)

Follow these steps to add *physical links* or *nodes* to an existing entity group from the Managed Objects tab. You can add *probes* to existing probe groups on the Probes Details Tab accessed from the Probes tab.

Prerequisite

You must first create groups before you can add entities to them; for details, see To Create a Group.

1. Click the Managed Objects tab.
2. In the Entity Type drop-down menu, select **Physical Links** or **Nodes**.
3. In the first column in the Managed Elements Pane, click the check boxes next to the entities you want to add to the entity group.
4. Click the **Add to Group** button. The Add to Group dialog box appears.
5. Select the name of the group you created previously and click the **Add to Group** button. A message appears confirming the number of entities that were added to the group.
6. Click the Groups tab to display the Groups Pane and verify that the entities have been added to the group.

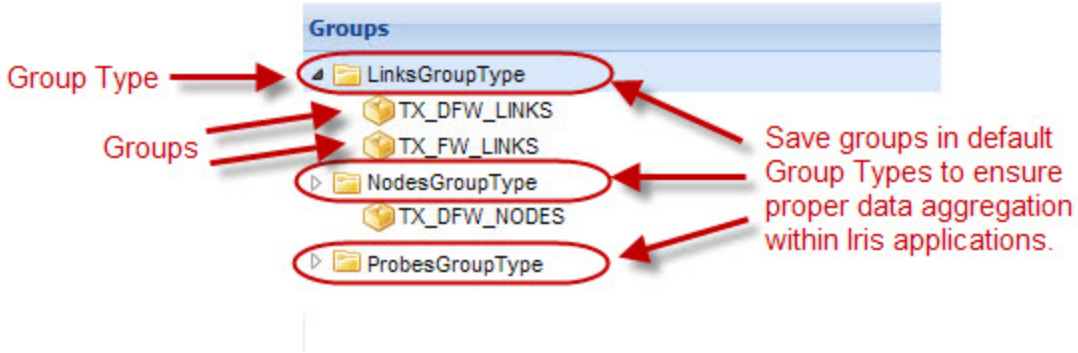
Entity Groups

After you configure entities, you can create logical groupings of these entities to enable precise group monitoring capabilities using the Iris applications. The current release only supports groups of *physical links*, *nodes*, or *probes*.

Iris entity groups are comprised of group types, groups, and entities. Group types contain one or more groups; groups contain one or more entity members (physical links, nodes, or probes).

Iris provides three default group types: LinksGroupType, NodesGroupType, and ProbesGroupType. Certain Iris applications aggregate data on specific entity groups; refer to Iris Entity Support for details about which Iris applications support specific entity groups. To ensure proper data aggregation for these groups, Iris requires these groups reside in the default group types.

For example, ITA supports physical link groups and node groups. To view properly aggregated data within ITA for your defined groups, you must save the entity groups in the respective Iris system default group types: Link Groups and Node Groups.



Legacy Group Migration

Iris automatically migrates groups created prior to 7.11.2 (that is, legacy groups) into the appropriate default group type using the following logic:

- Iris categorizes legacy groups into the appropriate default group type using the originally defined name. For example, all legacy physical link groups are saved into the LinksGroupType.
- If a migrated legacy group is using characters other than those allowed, it is renamed to "Legacy-TIMESTAMP". Allowable characters include alphanumeric characters, minus (-), underscore (_), period (.), space ( ), colon (:), or slash (/). You can rename the group using the Edit option on the Groups Tab.

Configuring Traffic Classification

Traffic classification provides both protocol classification and application classification (either Tektronix-defined or user-configurable) throughout Iris applications. Operators can classify protocols and applications based on the following parameters:

- Protocols Based on IP/Port Combination
- Applications Based on IP/Port Combination
- Applications Based on URL or UA, and Content Type
  (Content-Type is predefined for MMS, http-video, http-audio, and is not user configurable)

You configure traffic classification on the Protocol Details pane and the Application Details pane on the Topology Tab. Refer to the ***Traffic Classification Configuration*** tutorial in the Admin online help for workflow details.

Topology Auto Detection

Iris Topology Management includes topology detection options that enable G10 probes to auto-detect network elements. When enabled, a probe automatically detects certain network elements that were previously provisioned manually by a network administrator. Topology auto-detection reduces the need to provide detailed information for provisioning and reduces the probability of provisioning errors, thus making the system more reliable.

Auto-Detection Controls

Iris provides the following auto-detection controls. As an alternate to node auto-detection, Iris also supports Staged Node Auto-Detection, where nodes can be detected by probes, but not added to the Topology database.

Setting	Location	What It Controls

Topology Detection Enabled	Admin Advanced Properties	Tektronix-controlled setting that enables/disables the auto-detection functionality on both the server and probe side. Contact Customer Support for assistance with this setting. The default setting is Disabled.
Auto Node Topology Commit Enabled Check Box	Probes Monitoring Details Tab	These settings enable/disable topology commits for **individual** probes. Controls whether new or updated nodes or links are automatically added to the Iris topology database or just logged. The default setting is Disabled. ***Note: These settings are ignored if the Topology Detection Enabled Admin advanced property is disabled.***
Auto Link Topology Commit Enabled Check Box		
Auto Node Topology Commit Enabled Check Box	Topology Auto Detection Tab	These settings enable/disable topology commits for **all** probes. ***Note: These settings are ignored if the Topology Detection Enabled Admin advanced property is disabled.***
Auto Link Topology Commit Enabled Check Box		

Node Detection

Iris designates each node as either a *per-probe* node or a *global* node for the purpose of determining how topology updates will be communicated to probes:

Per-probe Node

- A node that is explicitly designated by Tektronix as a per-probe node. *Currently, Iris only designates eNodeBs as per-probe nodes.*
- Per-probe node data is sent **only** to those probes to which the node is explicitly associated. *If an eNodeB is manually provisioned, it is not associated to a probe until a probe discovers it.*
- You can view the probes that are provisioned to each per-probe node in the Node Details tab.

Global Node

- A node that is **not** explicitly designated by Tektronix as a per-probe node.
- Global node data is sent to all G10 probes in the system.

See Iris Auto-Detected Elements for a list of nodes the G10 probes currently detect. All detected nodes appear in the Topology Management Tab on the Managed Objects Tab for nodes. You can edit individual nodes on the Node Details pane. You can edit multiple nodes at one time; refer to Using CSV File Import/Export for details.

See also Staged Node Auto-Detection.

Logical Link Detection

Iris determines whether a logical link is a *per-probe* link or a *per-probe* link for the purpose of determining how topology updates will be communicated to probes:

Per-probe Link

- If at least one endpoint is a per-probe node, then the link is implicitly a per-probe link.
- Per-probe link data is sent to only those probes to which their endpoint nodes are associated.
- You can view the probes that are provisioned to each per-probe node in the Node Details tab.

Global Link

- If both endpoints are global, the link is global.
- Global link data is sent to all probes in the system.

See Iris Auto-Detected Elements for a list of logical links the G10 probes currently detect. All detected links appear in the Topology Management Tab on the Managed Objects Tab for logical links. You can edit individual links on the Logical Link Details pane.

The two logical link endpoints are designated as server and client. The designation is protocol-specific, and typically the uplink node is the server (MME vs eNodeB in LTE, or GGSN vs SGSN on Gn interface). The direction of the packets on the links is set relative to the server node (RX is uplink, TX is downlink).

Node to Probe Association

Monitored Node to Probe Association

A node can be monitored by multiple probes and each probe can monitor multiple nodes. For topology and application processing efficiency, Iris identifies and maintains a node to probe association for monitoring purposes.

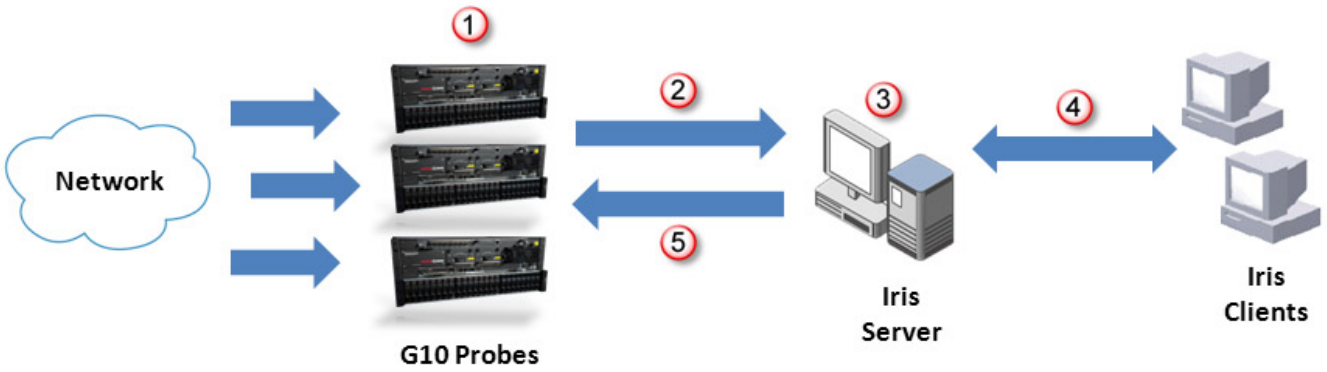
You can view node to probe associations in the following areas in Admin:

- Probe Management Tab - the Monitoring Details Tab lists the nodes a probe has observed in network traffic and is currently monitoring.
- Topology Management Tab - the Node Details pane lists the probes that have observed a node in network traffic and are currently monitoring it.

Provisioned Node to Probe Association

Iris also maintains a provisioned node to probe association for managing auto-detection updates for per-probe node types. A per-probe node is a node that is explicitly associated with at least one G10 probe. Per-probe node data is sent to **only** those probes to which it is explicitly associated. You can view the probes that are provisioned to each per-probe node in the Node Details tab.

Auto-detection Process



1	**G10 probes collect and process network data in real time, 24 hours a day, 7 days a week.** • When enabled, G10s perform network element detection based on incoming monitored traffic. • G10s determine network nodes and logical links by analyzing decoded PDUs.
2	**G10s forward auto-detected network element data to the Iris server.**

3	**If auto-topology commits are enabled, the Iris server processes new node discoveries from probes depending on the node designation (global or per-probe):** • **Global nodes:** merges auto-detected topology data from all probes and commits it to the master topology. • **Per-probe nodes:** Iris server associates nodes to the probes that discover them.
4	**The user views the master topology data on the Iris Admin GUI on the Iris Clients.** • User modifications to topology data through the Admin GUI are uploaded and merged into the master topology.
5	**The Iris server periodically downloads the topology updates depending on the node designation (global or per-probe):** • **Global node:** to all G10 probes that have auto-detection commits enabled. • **Per-probe nodes:** to only the G10 probes provisioned for that node that have auto-detection commits enabled.

Iris Auto-detected Elements

The following table shows the elements that Iris auto-detects.

Interface	Protocol	Node Detection?	Logical Link Detection?	Server Node
Gn	GTPv1-C	**None**	**Yes** SGSN<->GGSN/SGSN Gn logical links are only auto-detected if both SGSN and GGSN endpoints already exist in Topology.	N/A
S4	GTPv2-C	**Yes** SGSN SGW	**Yes** SGSN<->SGW S4 logical links are only auto-detected if both SGSN and SGW endpoints already exist in Topology.	N/A
S5/S8	GTPv2-C	**Yes** SGW PDN-GW	**Yes** SGW<->PDN-GW	PDN-GW
S10	GTPv2-C	**Yes** MME	**Yes** MME<->MME	N/A
S11	GTPv2-C	**Yes** MME SGW	**Yes** SGW<->MME	SGW
A11	A11	**Yes** ePCF HSGW	**Yes** ePCF<->HSGW	HSGW

Interface	Protocol	Node Detection?	Logical Link Detection?	Server Node
S1-MME	S1AP	**Yes** MME eNodeB	**Yes** eNodeB<->MME	MME
SIGTRAN	Sigtran	**Yes** Iris assigns all auto-detected SIGTRAN nodes with the SIGTRAN_NODE type. Use the Node Details pane to change the node type to a more descriptive SIGTRAN node type (such as SSP or STP). Iris saves either a point code or an IP address for each auto-detected SIGTRAN node. Use the Node Details pane to modify or add point code or IP address information. See also Combinational Nodes.	**Yes** Sigtran<->Sigtran	N/A

Auto-detected Node Names

The Iris server automatically provisions a name for auto-detected nodes using the "NodeType/IPAddress" or "NodeType/PointCode" syntax (such as "MME/1.1.1.1"). If multiple IP addresses or point codes are defined, the first IP address or point code is used for the naming scheme.

The Iris system can obtain carrier-provisioned equipment names for MMEs and eNodeBs automatically from certain broadcast network maintenance message types defined in Specification 3GPP 36.413:

Maintenance Message	3GPP 36.413 Reference	Information Element	Comment
S1 SETUP REQUEST	9.1.8.4	eNB Name	Optional eNB Name IE must be present
S1 SETUP RESPONSE	9.1.8.5	MME Name	Optional MME Name IE must be present
ENB CONFIGURATION UPDATE	9.1.8.7	eNB Name	Optional eNB Name IE must be present
MME CONFIGURATION UPDATE	9.1.8.10	MME Name	Optional MME Name IE must be present

When the Iris system detects one of these maintenance messages, it processes the nodes as follows:

Node Status	Current Name	New Name
Node does not exist in Iris system	N/A	New node uses carrier-provisioned name if Name IE is present

Node Status	Current Name	New Name
Node exists in Iris system	Iris auto-provisioned name "NodeType/IPAddress" or "NodeType/PointCode" syntax (such as "MME/1.1.1.1")	Renamed using carrier-provisioned name if Name IE is present
Node exists in Iris system	Custom node name	Node is not renamed

Staged Node Auto-Detection

As an alternative to Iris topology node auto-detection, Iris supports staged node auto-detection. This feature enables you to log auto-detected node data to a CSV file, rather than automatically provisioning the nodes in the topology database. By omitting these nodes from the topology database, they are not available for reporting purposes in Iris applications and DRs.

Admins can edit the CSV file and import the data into Iris and view the imported nodes in the Topology tab.

Configuration Settings

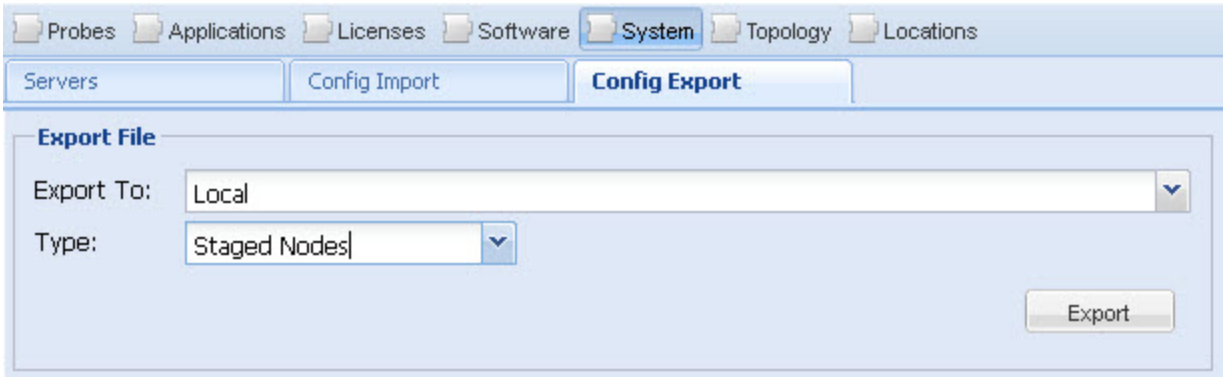
To ensure probes are auto-detecting nodes, but not auto-provisioning them in the topology database, the following configuration parameters should be set:

Setting	Location	Staged Node Setting
Topology Detection Enabled	Admin Advanced Properties	**Enable** this setting to auto-detect nodes and links on both the server and probe side. Contact Customer Support for assistance with this setting.
Auto Node Topology Commit Enabled Check Box	Probes Monitoring Details Tab	**Disable** topology commits for **individual** probes. New or updated nodes or links are only logged, and NOT automatically added to the Iris topology database.

Exporting/Reimporting Staged Node Data

- You can export the staged node data using the Config Export tab on the System tab.
  - Use the Staged Nodes option for the type of export. See Using CSV File Import/Export for details.
  - View the data in the StagedNodes-YYYY-MM-DD-hh-mm-ss.csv file. See CSV File Formats for details.
- Edit the CSV file and import the data using the Config Import tab on the System tab.

Config Export - Staged Nodes



Creating Domains in Topology Management

For cases in which aggregated IP traffic and Subscriber IP address reuse make it difficult to trace the origin of monitored IP packets, you can create domains, which are zones of VLAN IDs, physical links, and tap points within a network. ISA users can then filter ISA sessions by domain in the Network Page Probes View and Session page.

Capturing and filtering by Domain enables ISA users to perform the following functions:

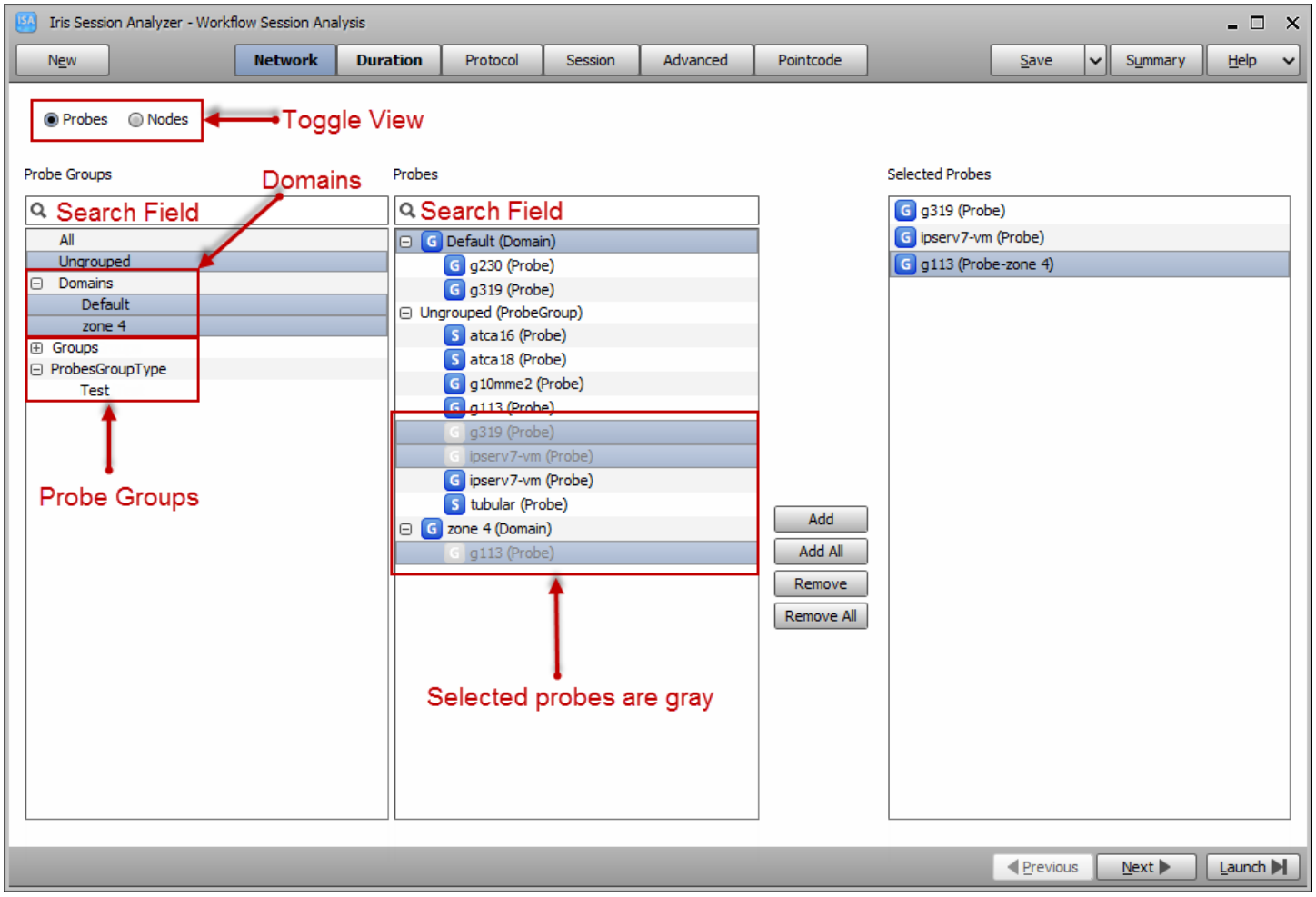
- Limit a session capture to a specific Domain
- Separate services in the network, such as voice and data (VoLTE)
- Capture voice only, data only, or both
- Capture MSIP traffic in a specific Domain
- Use node-based session filtering
- View Gi traffic and network elements such as firewalls, routers, and SBCs hop by hop
- View aggregated traffic separately in multiple physical links and Domains.

To Create a Domain

1. In the Managed Objects tab, select **Domains** from the Entity Type menu.
2. Click the **Add Entity** button.
3. In the Domain Details pane, enter a name in the Name field.
4. Click the ellipsis (**...**) next to the Anchor Node field to open the Anchor Node dialog box and add an anchor node, which must be a GGSN or PDN-GW.
5. Click the **Add** button to open the Select Physical Links dialog box from which you can select physical links for the Domain. You can assign VLAN IDs to physical links in the VLAN Assignment area of the Physical Link Details pane.
6. Click the **Save** button at the bottom of the Domain Details pane to save the new domain.

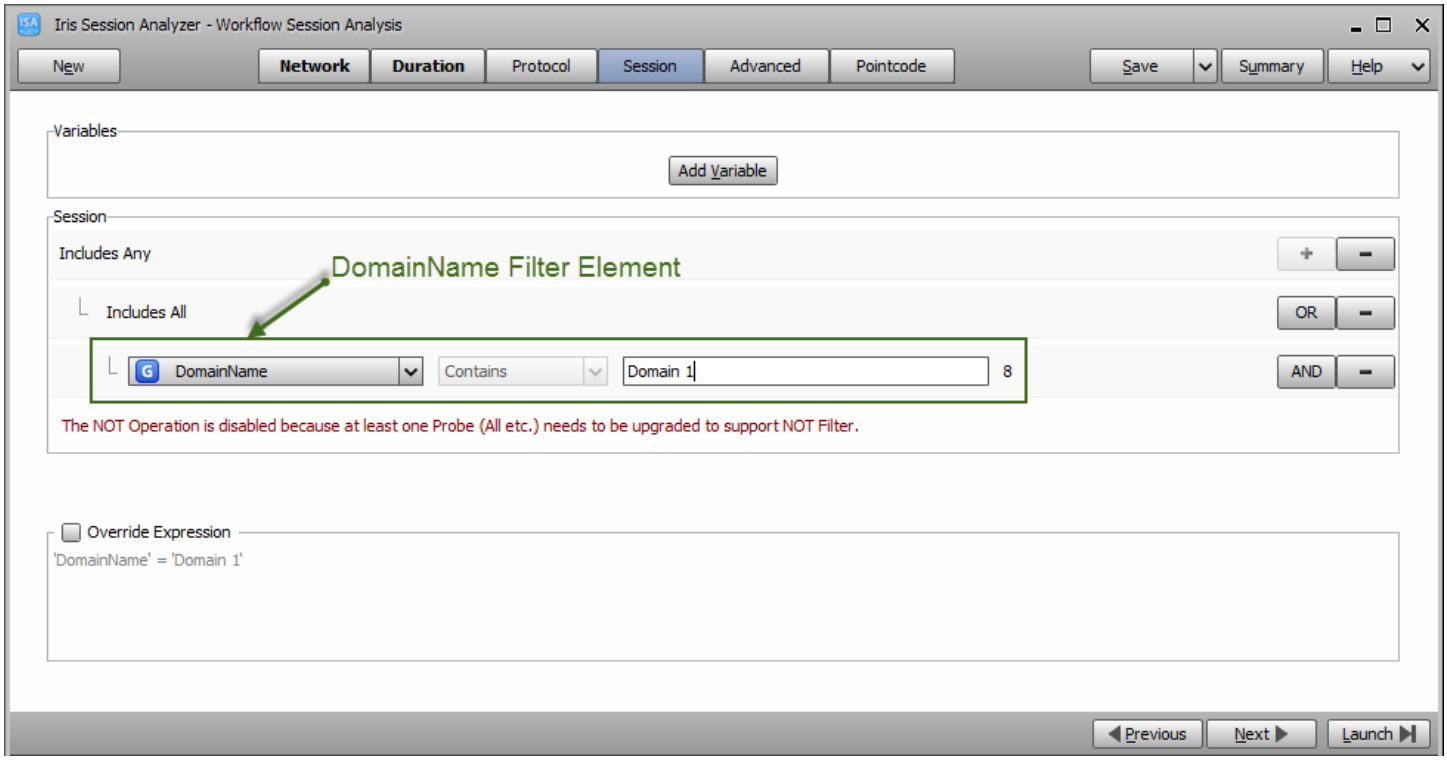
Domains in the ISA Network Page Probes View

Domains appear in the Probe Groups area within the Domains tree, along with the ProbesGroupType tree. When ISA users select one or more domain(s) from the Domain selection group and proceed through an ISA Workflow, only ISA sessions within the domain(s) are captured.



Domains in the ISA Session Page

ISA users can enter a domain name into the DomainName filter element field to filter by domain in the ISA Session page.



Chapter 5 Application Management

The Application Management feature enables administrators to manage configuration settings for Store to Disk, ISA, ITA, and XDR Profile Management.

The Application Management Tab enables you to perform the following tasks:

- Managing Iris Data Storage
- Configuring ISA Default Node Type Order
- Configuring ITA Dashlet Display

Refer to XDR Profile Management in Chapter 7 for details about configuring data records.

Managing Iris Data Storage

Iris' Store to Disk Tab on the Applications Tab enables you to manage how data is stored to the disk arrays. The data can be recalled later using the PA and ISA applications. The Store to Disk options enable you to:

- Control which protocol PDU data is captured and stored to the disk array.
- Assign which disk volume protocol PDU data is stored (long-term or short-term).
- Configure which protocol PDU data is truncated prior to being stored to disk. See IP Packet Truncation for details. The truncated data can be viewed using the Protocol Analyzer application. Refer to the Iris Online Help for more details about viewing truncated packets.

You configure these settings in customized profiles that can be applied to individual probes in the Probes Tab.

To Create a Store to Disk Profile

You can create a completely new store to disk filter profile or use an existing profile as a template to create a new one.

1. Click the Applications tab and then click the Store to Disk tab. The Store to Disk Tab page appears.
2. Perform one of the following actions:
    - To create a new S2D filter profile, click the **New** button in the Profile List Pane. In the New Profile dialog box, enter a name for the profile and click **Create** to add the new profile to the list.
    - To use another profile as a template, select the profile you want to copy and click the **Copy** button. In the Copy Profile dialog box, enter a new name for the profile and click **Copy** to add the new profile to the list.
4. Select the new profile to display its settings in the Profile Detail Pane.

To Customize Store to Disk Settings

1. Clear any checkmarks in the Capture column for any protocols you do not want to capture and store on the disk array.
2. Place a checkmark in the corresponding cell of the Truncate column to enable packet truncation for that protocol. See IP Packet Truncation for details.
3. Click the corresponding cell in the Truncation Bytes column to enter the number of bytes to retain for each packet, prior to truncation (maximum value is 4095).

When enabling HTTP truncation, enter any non-zero value. The value set here does not control how HTTP truncation is managed by the G10; refer to IP Packet Truncation for details about how the G10 truncates HTTP packets.

4. Click the corresponding cell in the S2D Archive column and change the setting, as needed, to indicate the type of disk storage (Short Term, Long Term).

Changing a protocol's storage options (from LT to ST, or from ST to LT) will affect data accessibility for the PA client when users define capture filters. For example, if you change H.248 from Long Term to Short Term on July 20th 14:00, then all H.248 PDUs before July 20th 14:00 are saved in the LT archive, and all H.248 PDUs after July 20th 14:00 will be saved in the ST archive. When users define a capture filter for H.248, PA only searches ST after July 20th 14:00, so the H.248 data stored in G10 before July 20th 14:00 is not searched by PA. If the user does not define capture filters, PA searches both LT and ST archives.

In this scenario, if the user still needs to filter H.248 data stored on G10 before the ST/LT archive change, Tektronix can configure Iris to search both the LT and ST archives. Contact Customer Support for details.

5. Repeat Step 1 to Step 4 to customize the capture settings for additional protocols, and then click **Save**.
    - If modifying an existing profile, the changes are immediately uploaded to the probes that are assigned this profile.
    - If creating a new profile, you can assign to an individual probe.

To Assign a Store to Disk Profile to a Probe

1. Click the Probes Tab.
2. In the Probes Area, select a G10 probe to display its settings in the Probe Details Tab.
3. In the Probe Details tab, select the store to disk configuration for the probe.
4. Click **Save** To save the G10 probe settings.

Configuring ISA Default Node Type Order

You can set a system default to control the order in which node types appear in the ISA Ladder Diagram. Default node type order settings are system-wide and apply to all ISA users. The node type order system default is applied to the node types detected for a given session.

Details about this feature include:

- A Tektronix system default node type order, based on typical call flows, is installed with the system. Administrators can modify the node type order in the ISA Configuration tab and save it as the new system default setting.
- Default node type order settings are system-wide and apply to all ISA users. Users can override default settings and create and save their own custom node type order in the ISA Results window. Refer to the Iris Online Help for details.

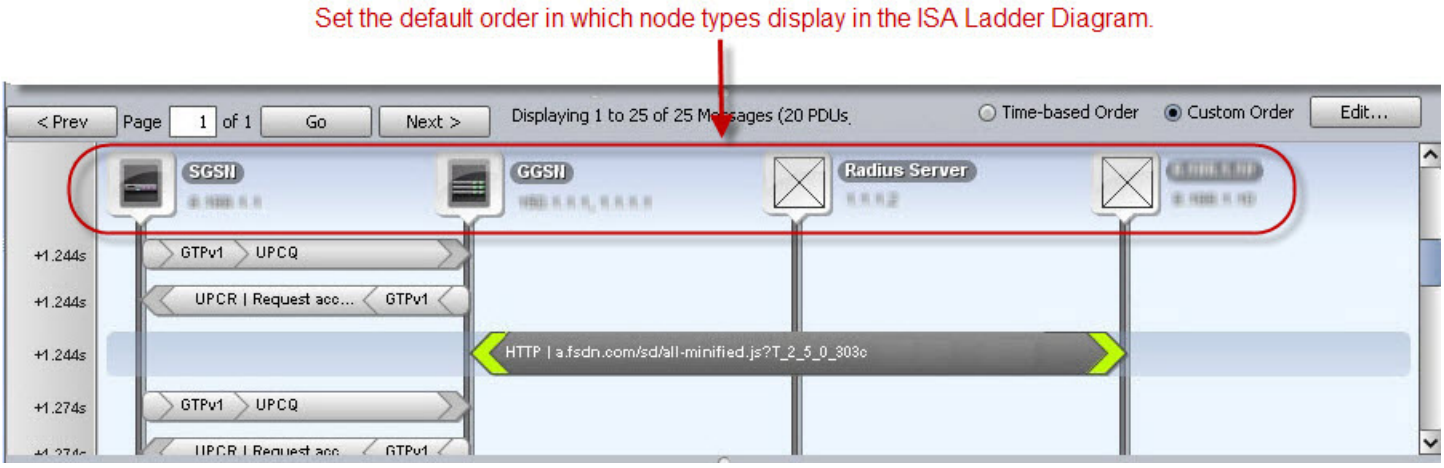
This feature applies to both G10 and Splprobe monitored node types.

To Set the Default ISA Node Type Order

1. Click the Applications tab, and then click the ISA Configuration tab. The ISA Configuration Tab page appears.
2. Use the Selection Control Buttons to:
    - Add and Remove node types to and from the Selected Pane. The node types included in the Selected pane control the node type order in the ISA Ladder Diagram.
    - Adjust the order of node types in the Selected list pane to reflect the Node Type Order from left to right in the ISA Ladder Diagram.
3. Click the **Save** button to save your changes as the default node type order or click the **Cancel** button to revert back to the Tektronix system default node order.

    Any modifications you make to the default do not take effect until ISA is restarted or the user changes the system default order in the ISA Results window. Refer to the Iris Online Help for details.

ISA Ladder Diagram in Results Window



Configuring ITA Dashlet Display

You can set system-wide defaults for certain ITA Dashlets to control select display settings. The ITA Configuration tab enables you to configure the following settings:

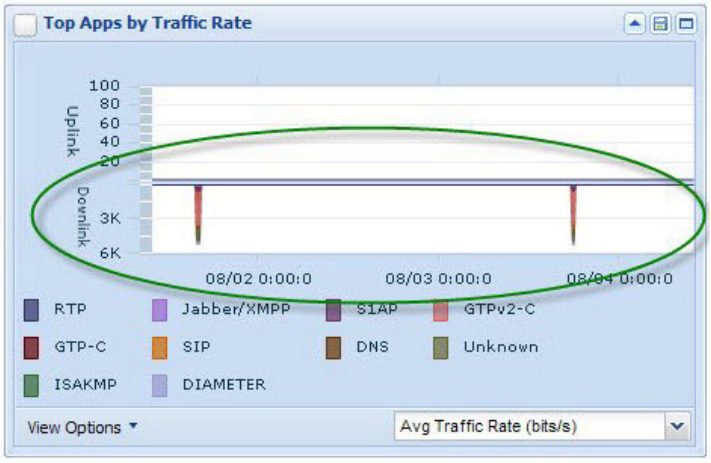
- Configure the appearance of the Nodes by Volume dashlet in ITA.
- Configure the default appearance of downlink traffic in certain ITA dashlets.

To Customize ITA Dashlet Display

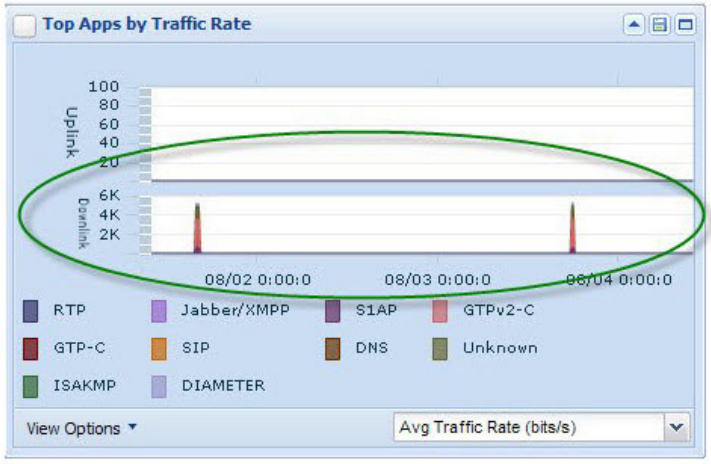
1. Click the Applications tab, and then click the ITA Configuration tab. The ITA Configuration Tab page appears.
2. Enter a new Top N Value for ITA users for the Nodes by Volume dashlet. The value cannot exceed the Tektronix configured maximum; contact Customer Support for details.
3. Select **Standard** to change the appearance of downlink traffic in certain ITA dashlets. By default, downlink traffic displays as Inverted. Refer to the Iris Online Help for details on which dashlets this setting affects.
4. Click the **Save** button to save your changes as the default or click the **Reset** button to revert back to the Tektronix system default.

   The new settings only apply to new users created after the defaults are modified. Users can override the default settings by changing their Preferences from the ITA Dashboard. Refer to the Iris Online Help for details.

Standard vs. Inverted Display Example



Inverted Display



Standard Display

Chapter 6 System Maintenance

This chapter provides information about the tasks associated with the Admin System tab and the Software tab.

- Define servers
- CSV Import/Export

The Software Tab enables you to manage updates for G10 and gSoft RAN probes and TD140 devices:

- Upgrading Probe Software
- Upgrading TD140 Software
- Upgrading G10 Probe and Array Firmware

Defining Servers

You can define the various servers the Iris server needs to communicate with using the Servers tab. The servers you need to define vary depending on deployed applications and probes.

To Define Servers

1. Click the **System Tab** to display the System Properties - Servers page.
2. In the **NTP server** area, enter up to 11 IP addresses (IPv4 or IPv6) for the NTP servers that will synchronize timing across all G10 probes and Iris servers. Separate IP addresses with commas. Each defined IP address appears as an option in the NTP Server field in the Timing Control Tab.

   Tektronix Communications recommends provisioning three or more servers as a best practice for reliability of timing references.

3. In the **GeoProbe Adapter server** field, enter an IP address for the SpIserver. This field is required when the ISA or Maps applications are deployed with SpIprobes.
4. In the **Geo/Spi Server Host** field, enter an IP address for the SpIserver. This field is required to support applications deployed with SpIprobes.
5. In the **Geo Cas Server Hostname** field, enter a hostname for the SpIserver on which the GeoProbe CAS resides. This field is required when the PA application is deployed with SpIprobes. N/A indicates an Iris-only deployment.
6. In the **NGGEO Jboss Server Hostname** field, enter a hostname for the SpIserver on which Jboss resides. This field is required when the PA application is deployed with SpIprobes. N/A indicates an Iris-only deployment.
7. In the **PTP Server** field, enter an IP address for the PTP server you want the TD140 to use for synchronization. The address listed here is listed in the TD140 Details tab. A TD140 can only be assigned one PTP server.
8. To save the settings, click **Save**.

Using CSV File Import/Export

Iris supports an Import and Export feature on the System Tab that enables bulk import/export of CSV files. The utility exports data to a CSV-formatted file that can be edited in any text editor or Microsoft Excel. The updated file can then be imported back into the Iris system for bulk updates.

The Import feature also supports importing trunk mapping tables; refer to Enabling ISUP H248/MGCP Correlation for ISA.

Follow these steps to manage CSV data using the Config Import and Config Export tabs.

To Export CSV Data

If you are exporting data from a system other than Iris, you must add a header row using specific column headings; see CSV File Formats for details. You can add the column headings in any order to match the order of your exported data.

1. Click the System Tab, then click the **Config Export** tab.
2. Select a location to export the CSV file to: **Server** or **Local**.
   - Server - define the server directory in the Server field.
   - Local - you are prompted to select a location on your local drive when you select Save.
3. Select the entity type you want to export from the **Type** drop-down menu.

You can export protocol and probe data for reference purposes only; you cannot reimport these data files.

4. Click the **Export** button. The file is saved with following name syntax: `[Type]-yyyy-MM-dd-HH-mm-ss.csv`. Refer to CSV File Formats for details.
   - Server - Iris exports data to the default directory on the Iris server.
   - Local - select a directory on your local drive to save the data.

To Modify Exported CSV Data

5. Access the file on the Iris server and modify the data using any text editor or Microsoft Excel. See Node Import Actions or Application Import Actions for details. Contact Customer Support if you need assistance accessing the Iris server.
6. Save the file to the /export0/home/iris directory on the Iris server; ensure it is in .csv format. Contact Customer Support if you need assistance accessing the Iris server.

To Reimport Modified Entity Data

7. From IrisView, click **Admin** and then click the System Tab.
8. Click the **Config Import** tab.
9. Use the default source directory, or enter the source directory where the CSV files reside and click the **Change Directory** button. CSV files residing in the directory display in the File list.
10. Select the check boxes of the CSV files you want to import. You can only select multiple files of the same type for import, not different types. For example, you can import multiple Application CSV files, but you cannot import an Application CSV file and a Node CSV file at the same time.
11. Click the **Import** button. View status and error messages in the Latest Import Log Pane. View processed entity statistics in the Latest Import Summary Pane.
12. Review errors and create a new CSV file to resolve any issues.
13. Click the Managed Objects Tab to verify entity updates in the Iris system. You can update Node Details and Application Details using the GUI if necessary.

Node Import Actions

You control what action to perform on a node by editing the values in the CSV file. You then reimport them into Iris to perform bulk entity updates. You can edit the CSV file in any text editor or in Microsoft Excel. See Using CSV File Import/Export for

details.

- Add New Nodes
- Modify Existing Nodes Using NodeID Lookup
- Modify Existing Nodes Using Name Lookup
- Delete Existing Nodes (Nodes with IP addresses only)
- Delete Existing Nodes (Nodes with Point Codes)
- Rename Existing Nodes

Node Import Required Columns

Column Name	Valid Values	Comment
ProbeId	Name of the probe associated with this node or empty	***The ProbeId field is used for informational purposes only; you cannot use this field to build new probe-to-node associations. The import function ignores this field, even if populated with fields from export.***
NodeId	Numeric ID of the node, 0 value, or empty	If empty or 0 value, OAM will try to add/merge this node into system
NodeType	Any supported node type	
NodeName	Unique node name or empty	If empty, the Iris server automatically generates a name using the "NodeType/IPAddress" or "NodeType/PointCode" syntax. If multiple IP addresses or point codes are defined, the first IP address or point code is used for the naming scheme.
IpAddresses	Must be in a valid IPv4 or IPv6 IP address format.	Can be empty for SIGTRAN node types, in this case node pointcodes should be provided.

Node Import Optional Columns

Column Name	Valid Values	Comment
Action	D - Delete R - Rename N - Modify Node using Name Lookup	See following sections: • Delete Existing Nodes (Nodes with Point Codes) • Rename Existing Nodes • Modify Existing Nodes Using Name Lookup
Groups	The group names to assign to this node.	Multiple group names should be wrapped in quotes and separated by a comma.

Column Name	Valid Values	Comment
PointCodes	PointCodes field must use the following format: "{{POINTCODE1,PROTOCOL,NETWORKINDICATOR}, {POINTCODE2,PROTOCOL,NETWORKINDICATOR}}" Point codes must be in a valid format pattern for their corresponding Network Indicator and Protocol. Default point code formats are defined by Tektronix based on protocol (ANSI, ITU) and Network Indicator. You can customize point code formats based on your network requirements; contact Customer Support for details.	Only applies to select node types
GUMMEI	Valid GUMMEI format: NNN-NNN-NNNNN-NNN. Example: 111-222-11222-44	Globally Unique MME identifier. Used to identify MME node.
eNodeBId	Numeric value: 0-1048575	eNodeB identifier within mobile operator network.
PhysicalLinks	Format: "ID1,ID2"	This parameter does not apply to Sigtran nodes. Only applies to nodes sharing an IP address, such as active/standby nodes. See Active/Standby Node Provisioning for details. This field is only included if at least one node has associated physical links; if all nodes in the database have no physical IDs associated to them, this field is not included in the export.
ITAEnabled	Y/N	Whether or not this node is monitored by the ITA application.

Add New Nodes

When adding a node, the bold fields require values in the CSV file entries (the remaining fields can be empty). Set the NodeId value to 0 or leave empty to indicate to Iris to add a new node.

ProbeId	**NodeId**	**NodeType**	NodeName	**IpAddresses**	Groups	PointCodes	GUMMEI	Physical Links

NodeId=0 or empty

NodeType must be a supported node type.

IpAddresses must be in a valid IPv4 or IPv6 IP address format. When importing new nodes, see also Automatic Node Merging.

Add Node Example 1

New MME Node added with auto-generated name "MME/1.1.1.1" and IP address 1.1.1.1.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	0	MME		1.1.1.1	

Add Node Example 2

New DNS Server named "DNS_FW" is added with defined IP addresses 1.1.1.1 and 2.2.2.2, and is added to TX_FW_NODES group.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	0	DNS	DNS_FW	"1.1.1.1,2.2.2.2"	"TX_FW_NODES"

Add Node Example 3

New STP node named "SIGTRAN_STP" is added with defined point codes 1-1-1 and 2-2-2 with corresponding protocol and network indicator data.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes
	0	STP	SIGTRAN_STP			"{{1-1-1,ANSI,International},{2-2-2,ANSI,International}}"

Add Node Example 4

New MME node named "MME_345" is added with defined IP addresses 6.6.6.6 and 7.7.7.7, and a defined GUMMEI of 555-65-44-10.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups	GUMMEI
	0	MME	MME_345	"6.6.6.6,7.7.7.7"		555-65-45432-10

Modify Existing Nodes Using NodeID Lookup

Use this method to modify nodes for which you know the NodeIds and you want to change any of the following parameters: NodeName, IpAddresses, PointCodes, and Group fields. The bold fields require values in the CSV file entries (the remaining fields can be empty):

ProbeId	**NodeId**	**NodeType**	**NodeName**	**IpAddresses**	Groups	PointCodes

NodeId must be a valid ID of an existing node.

NodeType must be a supported node type. ***The node type of an existing node cannot be modified using the bulk import utility; you must change the node type from the Topology Tab***. Refer to Configuring Nodes for details.

NodeName cannot exceed 63 characters.

- If modifying **NodeName**, the new name must be unique.
- If modifying **IpAddresses OR Point Codes**, existing NodeName must be present.

IpAddresses must be in a valid IPv4 or IPv6 IP address format. When importing new nodes, see also Automatic Node Merging.

Modify Node Example 1

NodeName and IPAddresses fields defined in import file overwrite existing MME Node (ID 965) in system.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	965	MME	DAL_MME	2.2.2.2	

Modify Node Example 2

NodeName and IPAddresses fields defined in import file overwrite existing MME Node (ID 965) in system. Modified node is also added to TX_DAL_NODES group.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	965	MME	DAL_MME	2.2.2.2	"TX_DAL_NODES"

Modify Node Example 3

Error. NodeName field is required when modifying IpAddresses.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	965	MME		3.3.3.3	

Modify Node Example 4

SIGTRAN_NODE_DFW was previously auto-detected and saved with 4.4.4.4 IP address. Point codes defined in the import file are added to the node.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes
	1010	SIGTRAN_ NODE	SIGTRAN_NODE_ DFW	4.4.4.4		{{1-1-1,ANSI,NATIONAL},{2-2-2,ANSI,NATIONAL}}

Modify Existing Nodes Using Name Lookup

Use this method to modify nodes for which you know the names; you do not have to know the NodeId using this method.

When modifying existing nodes using this method, only the IpAddresses, PointCodes, Physical Links, and Group fields can be updated.

You must insert an Action column (you can insert anywhere). The bold fields require values in the CSV file entries (the remaining fields can be empty).

ProbeId	Action	NodeId	**NodeType**	**NodeName**	**IpAddresses**	Groups	PointCodes	Physical Links

Action=N

NodeId must be a valid ID of an existing node or empty.

NodeType must be a supported node type or empty. ***The node type of an existing node cannot be modified using the bulk import utility; you must change the node type from the Topology Tab***. Refer to Configuring Nodes for details.

NodeName must be valid name of existing node.

- If a node with this name is NOT found, the row will be imported as a new node, if it passes IPAddresses+Physical links validation.
- If the node with this name IS found, IP range+PhysicalLinks validation is performed:
  - If it conflicts with an existing node, an error is logged and the row is ignored. The error message contains details about the conflicts.
  - If it does NOT conflict with an existing node, then the node's IpAddresses, PointCodes, Physical Links, and Group values are overwritten with those defined in the CSV file.

IpAddresses must be in a valid IPv4 or IPv6 IP address format. When importing new nodes, see also Automatic Node Merging.

Modify Node Example 1

After validating DAL_MME exists, the IPAddresses and Groups fields defined in import file overwrite existing MME Node in system.

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups
	N		MME	DAL_MME	4.4.4.4	DALLAS

Delete Existing Nodes (Nodes with IP addresses only)

When deleting existing nodes that support only IP addresses, a value is only required in the **NodeId** field. An empty IpAddresses field indicates to Iris to delete the node.

ProbeId	**NodeId**	NodeType	NodeName	IpAddresses	Groups

- **NodeId** must be a valid ID of an existing node.
- Remove values from the **IpAddresses** field

Delete Node Example 1

Node (ID 965) is deleted from the system.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	965				

Delete Node Example 2

Node (ID 965) is deleted from the system.

ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups
	965	MME	DAL_MME		

Delete Existing Nodes (Nodes with Point Codes)

When deleting existing nodes that support point codes and IP addresses, you must insert an Action column (you can insert anywhere). The bold fields require values in the CSV file entries (the remaining fields can be empty).

ProbeId	**Action**	**NodeId**	NodeType	NodeName	IpAddresses	Groups	PointCodes

- **NodeId** must be a valid ID of an existing node that supports point codes.
- **Action**=D

Delete Node Example 1

Node (ID 1010) is deleted from the system.

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes
	D	1010					

Delete Node Example 2

Node (ID 1010) is deleted from the system.

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes
	D	1010	SIGTRAN_ NODE	SIGTRAN_ NODE_DFW	4.4.4.4		{{1-1-1,ANSI,NATIONAL},{2-2-2,ANSI,NATIONAL}}

Rename Existing Nodes

Note: *The Iris system can auto-detect carrier-provisioned node names for MMEs and eNodeBs from certain broadcast network maintenance message types; refer to Auto-detected Node Names for details.*

When renaming existing nodes, you must insert an Action column (you can insert anywhere). The bold fields require values in the CSV file entries (the remaining fields can be empty). ***When renaming nodes, the NodeID field must be empty.***

ProbeId	**Action**	NodeId	NodeType	**NodeName**	**IpAddresses**	Groups

- New **NodeName** must be unique.
- For nodes having IP addresses, the **IpAddresses** field must contain a valid IP address of an existing node and cannot contain a range.
- **Action**=R

Rename Node Example 1

Existing MME Node with IP address 1.1.1.1 is renamed to "MME_SW".

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups
	R			MME_SW	1.1.1.1	

Rename Node Example 2

Error. NodeId must be empty (remove NodeId "956") for the rename action to work properly for nodes having IP addresses.

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups
	R	956		MME_SW	1.1.1.1	

Rename Node Example 3

Existing SIGTRAN_NODE with IP address 4.4.4.4 is renamed to "SIGTRAN_DFW_45".

ProbeId	Action	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes
	R		SIGTRAN_ NODE	SIGTRAN_ DFW_45	4.4.4.4		{{1-1-1,ANSI,NATIONAL},{2-2-2,ANSI,NATIONAL}}

Application Import Actions

You control what action to perform on an application by editing the values in the CSV file. You then reimport them into Iris to perform bulk entity updates. You can edit the CSV file in any text editor or in Microsoft Excel. See Using CSV File Import/Export for details.

- Add New Applications
- Modify Existing Applications

- Delete Existing Applications

Add New Applications

When adding an application, the bold fields require values in the CSV file entries (remaining fields can be empty):

ID	**Name**	LongName	Enabled	**URL**	**UA**	**IpPortRanges**

- **ID**=0
- **Name** must be unique to applications and protocols and in enclosed in quotation marks
- **URL**, **UA**,**IpPortRanges**- either URL/UAs or IP Addresses/Port values must be defined for an application
  - **URL/UA**s must use "URL1,URL2","UA1,UA2" format. If null, leave the field blank (do not use ""). See Application Details Pane for additional format details.
  - **IpPortRanges** must use following format: [{'IPAddress1,IPAddress2','Protocol','Ports'}, {'IPAddress1,IPAddress2','Protocol','Ports'}]. See Application Details Pane for additional format details.

Add New Application Example 1

A new user-defined application for video is added with defined IP/Port ranges.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
0	"Video-App"	""	true			"[{'*','TCP','6565'},{'1.1.1.1,2.2.2.2','UDP','6565'}]"

Add New Application Example 2

A new user-defined application is added with news URLs.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
0	"MSNBC"	"MSNBC News"	true	"msnbc.com,msnbc.*/page"		

Modify Existing Applications

When modifying existing applications, the bold fields require values in the CSV file entries (the remaining fields can be empty). ***For Tektronix-defined applications, you can only modify Name, LongName, Enabled, and IpPortRanges fields; you cannot add/modify URL/UA parameters to Tektronix-defined applications.***

ID	Name	LongName	Enabled	**URL**	**UA**	**IpPortRanges**

- **ID** must be a valid ID of an existing application
- **URL, UA, IpPortRanges**
  - **URL/UA**s of user-defined applications must use "URL1,URL2","UA1,UA2" format. If null, leave the field blank (do not use ""). See Application Details Pane for additional format details.
  - **IpPortRanges** must use following format: [{'IPAddress1,IPAddress2','Protocol','Ports'}, {'IPAddress1,IPAddress2','Protocol','Ports'}]. See Application Details Pane for additional format details. You can add or modify IpPortRanges for both user-defined and Tektronix defined applications

Modify Application Example 1

IpPortRanges fields defined in import file overwrite existing Video-App application (ID 63002) in system.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
63002	"Video-App"	""	true			"[{'*','TCP','6565'}]"

Modify Application Example 2

URL fields defined in import file overwrite existing WSJ-Digital application (ID 63010) in system.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
63010	"WSJ-Digital"	"Wall Street Journal"	true	"online.wsj.com/home-page,marketwatch.com"		""

Delete Existing Applications

When deleting existing applications, only the **ID** field is required. Empty URL, UA, and IpPortRanges fields indicates to Iris to delete the application. ***You cannot delete Tektronix predefined applications such as Google or Facebook.***

ID	Name	LongName	Enabled	URL	UA	IpPortRanges

- **ID** must be a valid ID of an existing application.
- Remove values from the **URL**, **UA**, **IpPortRanges** fields (leave quotation marks for IpPortRanges) to indicate to Iris to delete the application.

Delete Application Example 1

Application (ID 63002) is deleted from the system.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
63002	"Video-App"	""	true			""

Delete Application Example 2

Application (ID 63010) is deleted from the system.

ID	Name	LongName	Enabled	URL	UA	IpPortRanges
63010	"WSJ-Digital"	"Wall Street Journal"				""

CSV File Formats

Iris supports the import and export of the following types of CSV files using the Topology Import/Export feature.

CSV File	Iris Export	Iris Import
Application Data	X	X
Domain Data	X	X
Node Data	X	X
Protocol Data	X	
Probe Data	X	
Staged Node Data	X	X
Trunk Mapping		X

The Topology Import feature also supports CSV files not created using the Topology Export feature. These files must reside on the Iris server and conform to specific formats for successful entity import.

For details about importing nodes and applications, see Node Import Actions and Application Import Actions.

CSV File Column Headings

CSV files are exported with specific column headings. If you are exporting data from a system other than Iris, *you must add the column headings as the first line in the CSV file*. You can add the column headings in any order to match the order of your exported data columns.

For trunk mapping, the column heading line should begin with the # symbol so that it is ignored as a comment.

Node CSV File Format

#Exported by Server at Thu Sep 01 22:24:56 UTC 2011								
ProbeId	NodeId	NodeType	NodeName	IpAddresses	Groups	PointCodes	GUMMEI	Physical Links
	1	AS	000004_NODEB	3.3.3.3				
	2	SGSN	SGSN_214	"1.2.3.4, 1.2.3.6"				
	3	eNodeB	000003_NODEA	1.2.3.4				
	4	eNodeB	000004_WEST	"4.4.4.4, 5.5.5.5"				
	5	eNodeB	000005_SOUTH	6.6.6.6	"TX_ DFW_ NODES"			
	6	SIGTRAN_ NODE	SIGTRAN_ NODE/111-111-001			{{002-110-001, ANSI,NATIONAL}}		
	7	SIGTRAN_ NODE	SIGTRAN_DAL	1.1.1.1				
"PROBE1"	8	MME	MME_FW	2.2.2.2			111-222-333-444	

Export Server Timestamp	Lists the name of the Iris server which exported the CSV file and the timestamp of when the file was created.
Column Headings	Lists the required column heading names: ProbeId,NodeId,NodeType,NodeName,IpAddresses,Groups **This line is mandatory for import. Columns may appear in any order. Optional columns: Action, PointCodes, and GUMMEI.**
ProbeId	This field is populated with the IDs of all probes associated with the node (if it is a per-probe node). Format: "PROBE1"
NodeId	An internal unique identifier for the node used by the Iris server.
NodeType	Text string identifying the type of node.
NodeName	Lists the defined node name.
IpAddresses	A list of valid IPv4 or IPv6 IP addresses and/or IPv4 IP ranges for the node. Multiple IP addresses are separated by a comma and enclosed in quotation marks. See Supported IP Address Formats and Syntax for details.
Groups	Names of groups the entity is a member. Format: "GROUP1,GROUP2"

PointCodes	Lists one or more point codes defined for the node. This field is only included if node types that support point codes exist in the topology. Formats: "{{POINTCODE,PROTOCOL,NETWORKINDICATOR}}" "{{POINTCODE1,PROTOCOL,NETWORKINDICATOR}, {POINTCODE2,PROTOCOL,NETWORKINDICATOR}}"
GUMMEI	Lists the unique GUMMEI defined for the MME node. This field is only included if MMEs exist in the topology. Format: NNN-NNN-NNNNN-NNN
Physical Links	Lists the physical link IDs that are assigned to this node. This field is only included if at least one node has associated physical links; if all nodes in the database have no physical IDs associated to them, this field is not included in the export. Format: "ID1,ID2" ***This feature does not apply to SIGTRAN nodes.***
Action	Optional column you can add for node import that allows the following actions. You can add the Action column in any location. Add one of the following letters: • R - Rename an existing node. • D - Delete an existing node that supports point codes. ***This action only applies to node types that support point codes.*** • N - Modify a node using its name as a lookup (rather than NodeId).

Staged Nodes CSV File Format

Staged Node CSV files can be edited and imported.

#Exported by Server at Fri Aug 30 13:55:44 UTC 2013							
ProbeID	NodeId	NodeType	NodeName	IPAddress	Groups	ITAEnabled	Count
probe123	0	MME		"1.1.1.1, 2.2.2.2"		Y	4
probe 456	0	eNodeB		"3.3.3.3, 4.4.4.4"		N	1
probe789	0	eNodeB		5.5.5.5		N	1

Export Server Timestamp	Lists the name of the Iris server which exported the CSV file and the timestamp of when the file was created.
ProbeId	Contains the ID of the probe that detected the node. You cannot modify this value for import.
NodeId	This value will be 0 for detected nodes. The Iris server assigns NodeID when the file is imported to database. You cannot modify this value for import.
NodeType	Text string identifying the type of node. You can modify this field for import.
NodeName	This value will be blank; the Iris server does not auto-provision staged node names. You can modify this field for import.
IpAddresses	A list of valid IPv4 or IPv6 IP addresses and/or IPv4 IP ranges for the node. You can modify this field for import. Multiple IP addresses are separated by a comma and enclosed in quotation marks. See Supported IP Address Formats and Syntax for details.
Groups	This value will be blank. You can modify this field for import.
ITAEnabled	This value contains the default value for the detected node type. You can modify this field for import.
Count	Total number of times which the node was detected by probes. Nodes with high detection counts can be prioritized by provisioning teams. This value is ignored on import.

Application CSV File Format

#Applications exported at Mon May 23 20:10:28 UTC 2011						
ID	Name	LongName	Enabled	URL	UA	IpPortRanges
62012	"Yahoo"	"Yahoo"	true	""	""	""
63001	"MSNBC"	"MSNBC News"	true	"msnbc.com,msnbc.*/page"	""	""
63300	"Video-App"	"Video Applications"	true	""	""	"[{'*','TCP','9789'}, {'1.1.1.1,2.2.2.2','UDP','9789'}]"

Export Server Timestamp	Lists the timestamp of when the file was created.
Column Headings	Lists the required column heading names: ID,Name,LongName,Enabled,URL,UA,IpPortRanges **This line is mandatory for import. Columns may appear in any order.**
ID	An internal unique identifier for the application used by the Iris server.
Name	Lists the defined application name.
LongName	Lists the details provided in the Description column of the Application Details pane.
Enabled	Indicates whether or not Iris is monitoring traffic for this application.
URL	Lists all URL patterns for user-defined applications; URL patterns for Tektronix-defined applications are not exported. URLs are separated by commas and enclosed in quotation marks.
UA	Lists all UA patterns for user-defined applications; UA patterns for Tektronix-defined applications are not exported. UAs are separated by commas and enclosed in quotation marks.
IpPortRanges	Lists all defined IP Address and Port combinations. Format: [{IPAddresses,'Protocol','Ports'},{IPAddresses,'Protocol','Ports'}]

Protocol CSV File Format

Protocol CSV files are for reference purposes only. You can only edit protocols using the Protocol Details pane; you cannot import edited protocol CSV files.

#Protocols exported Thu Sep 01 22:25:35 UTC 2011					
ID	Name	LongName	Enabled	Layer	IpPortRanges
67	DHCP	Dynamic Host Configuration Protocol	TRUE		"[{'','UDP','67,68'}]"
546	DHCPv6	Dynamic Host Configuration Protocol v6	TRUE		"[{'','UDP','546,547'}]"
3868	DIAMETER	DIAMETER Protocol	TRUE		"[{'','TCP','3868'}, {'','SCTP','3868'}]"
9	DISCARD	Discard Protocol	TRUE		"[{'','TCP','9'}, {'','UDP','9'}]"
20000	DNP3	Distributed Network Protocol	TRUE		"[{'','TCP','20000'}, {'','UDP','20000'}]"

Export Server Timestamp	Lists the timestamp of when the file was created.
Column Headings	Lists the column heading names: ID,Name,LongName,Enabled,Layer,IpPortRanges

ID	An internal unique identifier for the protocol used by the Iris server.
Name	Lists the defined protocol name.
LongName	Lists the details provided in the Description column of the Protocol Details GUI.
Enabled	Indicates whether or not Iris is monitoring traffic for this protocol.
Layer	List whether the protocol is categorized as Layer 3 (L3) or Layer 4 (L4).
IpPortRanges	Lists all defined IP Address and Port combinations. Format: [{IPAddresses,'Protocol','Ports'},{IPAddresses,'Protocol','Ports'}]

Probe CSV File Format

Probe CSV files are for reference purposes only. You can only edit probe data using the Probes Tab; you cannot import edited probe CSV files.

#Exported at Fri May 31 19:43:33 GMT 2013

ProbeId	ProbeName	IpAddress	Type	Status	Parent	Nodes Count	ENodeBs Count	IpAddresses Count	ItaEnabled Count	NodeAutoCommit Enabled	LinkAutoCommit Enabled	ISAProcessing Enabled	ISADisplay Enabled
4098	g312	1.2.3.4		DISCONNECTED									
4097	g110	1.1.1.1		DISCONNECTED									
4100	TD140 4100	2.2.2.2		NORMAL									
4103	g307	3.3.3.3		DISCONNECTED	4100								
4102	g313	4.4.4.4		NORMAL	4100								
4104	g307-1-1	6.6.6.6		DISCONNECTED									

Export Server Timestamp	Lists the timestamp of when the file was created.
Column Headings	Lists the column heading names: ProbeId,ProbeName,IpAddress,Type,Status,Parent
ProbeId	Unique number that identifies every provisioned probe.
ProbeName	Probe name configured on the Probe Details Pane.
IpAddress	IP address that was configured on the probe at installation.
Type	G10, TD140, or gSoft

Status	• Connected probes have one of the following statuses:
	  • NORMAL
	  • SOFTWARE_UPGRADE
	  • S2D_CONFIG
	  • SOFTWARE_UPLOAD
	  • SOFTWARE_REMOVE
	• MAINTENANCE status is controlled by the Maintenance State check box on the Probe Details Pane.
	• DISCONNECTED status indicates one or more device processes is down; see Connection Status.

Parent	This column does not appear in CSV file if no probes are bound to a TD140.

Nodes Count	Number of nodes this probe detected and is monitoring.
ENodeBsCount	Number of eNodeBs this probe detected and is monitoring.
IpAddressesCount	Number of IPaddresses this node detected and is monitoring. Note that an IP range counts as only one against the probe limit.
ItaEnabledCount	Number of nodes with ITA Enabled setting enabled (on Node Details Pane).
NodeAutoCommitEnabled (Y/N)	Probe's Auto Node Topology Commit Enabled setting (on probe Monitoring Details tab)
LinkAutoCommitEnabled (Y/N)	Probe's Auto Link Topology Commit Enabled setting (on probe Monitoring Details tab)
ISAProcessingEnabled (Y/N)	Probe's Session Tracking Enabled setting (on probe Monitoring Details tab)
ISADisplayEnabled (Y/N)	Probe's Session Tracking Display Enabled setting (on probe Monitoring Details tab)

Trunk Mapping CSV File Format

You cannot export trunk mapping data using the Topology Export feature. You must format the trunk mapping data using the following format. Iris does not require a specific filename syntax; it determines the type of data from the file content.

All columns are mandatory for trunk mapping. However, the column heading line should begin with the # symbol so that it is ignored as a comment.

#Protocol	Network Indicator	CA Point Code	Adjacent SP Point Code	Adjacent CIC	Termination ID
A	N	241-100-100	100-008-200	400	IIII0800.SS_2003_VT15_0114.1
A	N	241-100-100	100-008-200	401	IIII0800.SS_2003_VT15_0114.2

Protocol	A=ANSI I=ITU
Network Indicator	SS7 Network Indicator code for specified point codes N = National I = International NS = National Spare IS = International Spare
CA Point Code	The SS7 point code of the MGC, also known as the Call Agent (CA). The format of the point code must match the point code format identified by the combination of protocol and network indicator specified for the entry.
Adjacent SP Point Code	The SS7 point code for the signaling point (SP) adjacent to the Termination. The format of the point code must match the point code format identified by the combination of protocol and network indicator specified for the entry.
Adjacent CIC	The CIC adjacent to the Termination, specified as a decimal number.
Termination ID	The name corresponding to the Termination Identifier for this entry. The Termination ID is an ASCII string that cannot contain a comma or non-printable character. Duplicate Termination IDs are not allowed in the mapping table.

Domain CSV File Format

#Exported at Thu Dec 19 14:05:06 CST 2013			
DomainID	DomainName	AnchorNode	Action
2	zone4		
14	test16	test_14_2	
16	Domain13_2	test_13_2	
3	zone55	anchor-4	
4	zone5	anchor-1	
5	zone6		
10	zone7	anchor-2	
11	zone8	anchor-7	

DomainID	Internal Domain identifier IDs used by the Iris server and automatically generated when you create a Domain. Upon CSV file import, the Iris server takes the following actions depending on the absence or presence of the DomainID: • If a DomainID is absent in a row, the Iris server adds a new Domain entry with a new DomainID. • When a DomainID is present but there is no matching Domain in the system, the Iris server adds the Domain and generates a new DomainID.
DomainName	Change the name in the DomainName field to update the name in the system upon import.
AnchorNode	Change the name in the AnchorNode field and update the name in the system upon import.
Action	Enter a D when you want to delete a Domain. This field is optional.

Automatic Node Merging for New Node Import

The Node Import utility performs node merging logic when processing new nodes in CSV import files. A new node will be merged with an existing node having an IP address range if the following conditions are true:

- The new node's **Node Type** also matches the existing node.
- The new node's **IP Address** is NOT an IP Address range.
- The new node's **IP Address + Probe ID** is within one and only one existing node's IP range with the same Probe ID.

The following table shows examples of new and existing node definitions as well as the result of importing the new nodes into the system.

New Node Definition		Existing Node Definition		Result
Node Type	**IP Address**	**Node Type**	**IP Address**	
MME	"1.1.1.3, 2.2.2.5"	MME	1.1.1.1-1.1.1.4	New node is merged into existing node: MME, "1.1.1.1-1.1.1.4, 2.2.2.5"
MME	1.1.1.3-1.1.1.6	MME	1.1.1.1-1.1.1.5	Error message • Merge not allowed because new node definition contains an IP range • Row is skipped
MME	1.1.1.3	MME	1.1.1.4	New node is not merged, but added as a separate node. • Existing node definition does not contain an IP range • System does not merge nodes with adjacent IP addresses
MME	1.1.1.3	eNodeB	1.1.1.1-1.1.1.5	Error message • New node is different node type than existing node • IP address conflict for IP address range 1.1.1.1-1.1.1.5
MME	1.1.1.3 Probe ID: 1	MME	1.1.1.1-1.1.1.5 Probe ID: 1	New node is merged into existing node with probe ID 1.
MME	1.1.1.3 Probe ID: 1	MME	1.1.1.1-1.1.1.5 Probe ID: 2	MME 1.1.1.3 exists separately in the database; there is no IP address conflict since nodes have different Probe IDs

Enabling ISUP H248/MGCP Correlation for ISA

This procedure only applies to G10 probes. Refer to the GeoProbe product documentation for information regarding SpIprobe trunk mapping. Contact Customer Support for assistance in applying trunk mapping tables to SpIprobes.

When MGCP or H.248 signaling is used to control a Trunking Gateway interfacing an SS7 ISUP call leg, Iris requires a trunk mapping table to enable MGCP/ISUP and H.248/ISUP Multi-Protocol Correlation (MPC). For H248/MGCP sessions, Iris searches the mapping table by Termination ID to locate the proper point codes and Circuit Identification Code (CIC).

You must provide the trunk mapping data in a properly formatted CSV file. You import the file using the Config Import Tab, enabling Iris to process the trunk mapping definitions for ISUP H248/MGCP correlation.

Prerequisite

Verify the trunk mapping file is in the correct Trunk Mapping CSV file format. Copy the file to the Iris server; the default directory for importing files is /export0/home/iris. Contact Customer Support if you need assistance accessing the Iris server.

To Import a Trunk Mapping Table

1. Click the System Tab.
2. Click the **Config Import tab**.
3. Use the default source directory or enter the source directory where the CSV files reside and click the Change Directory button. CSV files residing in the directory display in the File list. Iris identifies the file type of each CSV file from its contents.
4. Select the check box of the trunk mapping CSV file you want to import. Iris supports importing and processing only one trunk mapping CSV file.
5. Click the **Import** button. View status and error messages in the Latest Import Log Pane. The total number of records processed in the CSV mapping file appears in the Total Processed field in the Latest Import Summary Pane.
6. Review errors and create a new CSV file if necessary to resolve any issues. Re-import the CSV file if necessary.

Upgrading Probe Software

PRIOR TO UPGRADING, YOU MUST READ ALL RELEASE NOTES AND UPGRADE CHECKLISTS TO ENSURE YOU ARE AWARE AND COMPLIANT WITH THE LATEST UPDATES TO THE UPGRADE PROCESS. FAILURE TO COMPLY WITH THE LATEST UPDATES COULD PROLONG THE PROBE UPGRADE PROCESS AND RESULT IN EXTENDED DOWN TIME. CONTACT CUSTOMER SUPPORT FOR ASSISTANCE.

G10 and gSoft RAN probe software is initially installed by Tektronix system engineers. You can perform subsequent probe software upgrades using the Software tab to create upgrade campaigns. A campaign is a defined set of configuration parameters for upgrading software packages for one or more probes. Campaigns enable you to:

- Perform individual probe or multi-probe software upgrades
- Upgrade both Platform and Application packages concurrently
- Schedule probe activation during non-peak hours

You can also view workflow details in the ***G10 Probe Software Upgrades*** tutorial in the Admin online help.

Upgrading G10 Probes Bound to a TD140

- The bound G10s are upgraded at the same time within one campaign; they cannot be upgraded individually.
- G10 probes bound to a TD140 device must be on the same version of software (EP and SP). The minimum software requirement is version 7.12.2.
- If a campaign failed on a managed G10 probe, a new campaign CANNOT be scheduled immediately. The user must wait until the previous campaign completes before scheduling a new one.

Prerequisites

Tektronix loads software upgrades on the Iris server to make them available for installation on the probes using probe campaigns. Available upgrades appear in the Software List pane on the Available Patches Tab.

Probes must have a minimum software version and Emergency Patch (EP) installed to support the version to be upgraded. Contact Customer Support for details.

For EPs requiring base versions, a probe campaign automatically loads the applicable base package with the EP if the base package resides on the Iris Server. You do not need to upload, install, or activate the base version prior to installing the EP. The Base package file (*.pit) must reside on the Iris server and appear in the Available Software Summary pane to be accessible for EP campaigns.

To Verify G10 Probe Software Packages

You must verify the software package integrity prior to updating probes. Follow these steps to verify software packages on the Iris server prior to installing on the probes.

1. Click the Software tab, and then click the Available Patches tab. Application and Platform software upgrades that were loaded on the Iris server are listed in the Software List pane.
   - Base and EP Application package files have a **.pit** extension.
   - Platform packages have a **.tgz** extension.
2. Select the package you want and click the **Verify** button.
   - If the package is valid, it is moved to the Available Software Summary Pane.
   - If the package cannot be verified, an error message displays and the package remains in the Software List Pane. Call Customer Support for assistance.
3. In the Available Software Summary Pane, verify the patch software has the correct version and date.

To Create a G10 Probe Software Upgrade Campaign

Once probe packages are verified, you can create a campaign to upload, install, and activate the software packages to one or more probes.

Probes must have a minimum software version and Emergency Patch (EP) installed to support the version to be upgraded. Contact Customer Support for details.

For EPs requiring base versions, a probe campaign automatically loads the applicable base package with the EP if the base package resides on the Iris Server. You do not need to upload, install, or activate the base version prior to installing the EP. The Base package file (*.pit) must reside on the Iris server and appear in the Available Software Summary pane to be accessible for EP campaigns.

Campaigns also support reverting back to a previous release of probe application or platform software. Previous release packages must be listed in the Available Patches Tab in order to be accessible for selection in revert campaigns.

Follow these steps to create a campaign for upgrading software on one or more G10 probes.

1. Click the Software tab, and then click the Probe Campaigns tab. The Campaigns pane appears.
2. Click **Add Campaign**; the Campaign Details Pane appears.
3. Select **G10 Probe** from the **Campaign Type** drop-down menu. Use this type for G10 probes and gSoft RAN probes.
4. Enter a name for the campaign.
5. Select a Platform and/or Application package for upgrading probes. You can choose from packages that have been verified and are listed in the Available Software Summary Pane on the Available Patches Tab.
6. Click the **Transfer Only** check box if you only want to transfer the packages from the Iris server to the probes and you do not want to activate them.
7. Select a date and time to activate the software packages. Tektronix recommends scheduling activation during non-peak hours. The probes require a reboot after activation and this process can take up to 10 minutes.
8. Click **Select Probes** to open the Probe Selector dialog box. Select a View option to filter the list.

   When scheduling any type of probe campaign (Transfer only, Activation only, and Transfer and Activation), the system administrator can include a maximum of 100 probes in the campaign. See Probe Campaign - Package Transfer and Activation for details about software package transfer and activation.

9. Select the check boxes for the probes you want to include in the campaign and click **OK**.
   - To upgrade all G10s bound to a TD140, select the TD140 check box.
   - You cannot select a probe for the campaign if it is disconnected, part of another current campaign, or running a Store-to-Disk (S2D) configuration.
   - The probes you select appear in the Probe Selection List in the Campaign Details Pane.
10. Verify your selections and click **Save**. A dialog box appears stating that the transfer will start immediately and asks you whether you want to continue.
11. Click **Yes** to confirm. The Iris server starts the transfer process. See Probe Campaign - Package Transfer and Activation for details about software package transfer and activation.

After activation, the probe(s) reboot. It may take up to 10 minutes for applications to shutdown before the probe(s) restart. Campaign and probe status will update to show success or failure. Monitor probe status in the Campaign Details Pane; monitor campaign status in the Campaigns Pane.

Upgrading TD140 Software

TD140 software is initially installed by Tektronix Communications system engineers. You can perform subsequent software upgrades using the Software tab to create upgrade campaigns. A campaign is a defined set of configuration parameters for upgrading software packages for one or more TD140s. Campaigns enable you to:

- Perform individual or multi-TD140 software upgrades
- Schedule TD140 activation during non-peak hours

Prerequisites

Tektronix Communications loads software upgrades on the Iris server to make them available for installation on the TD140 using campaigns. Available upgrades appear in the Software List pane on the Available Patches Tab.

To Verify TD140 Software Packages

You must verify the software package integrity prior to updating TD140. Follow these steps to verify software packages on the Iris server prior to installing them on the TD140s.

1. Click the Software tab, and then click the Available Patches tab. TD140 software upgrades that were loaded on the Iris server are listed in the Software List pane. TD140 Software package names will be in the format **TEKTD140.<version>.iso**
2. Select the package you want and click the **Verify** button.
   - If the package is valid, it is moved to the Available Software Summary Pane.
   - If the package cannot be verified, an error message displays and the package remains in the Software List Pane. Call Customer Support for assistance.
3. In the Available Software Summary Pane, verify the patch software has the correct version and date.

To Create a TD140 Probe Software Upgrade Campaign

Once TD140 packages are verified, you can create a campaign to upload, install, and activate the software packages to one or more TD140s.

Campaigns also support reverting back to a previous release of TD140 software. Previous release packages must be listed in the Available Patches Tab in order to be accessible for selection in revert campaigns.

Follow these steps to create a campaign for upgrading software on one or more TD140s.

1. Click the Software tab, and then click the Probe Campaigns tab. The Campaigns pane appears.
2. Click **Add Campaign**; the Campaign Details Pane appears.
3. Select **TD140 Device** from the Campaign Type drop-down menu.
4. Enter a name for the campaign.
5. Select a TD140 package. You can choose from packages that have been verified and are listed in the Available Software Summary Pane on the Available Patches Tab.
6. Click the **Transfer Only** check box if you only want to transfer the packages from the Iris server to the TD140 and you do not want to activate them.
7. Select a date and time to activate the software package. Tektronix Communications recommends scheduling activation during non-peak hours. The TD140s require a reboot after activation and this process can take up to 5 minutes. During reboot, the TD140 does not send heartbeats to the Iris Server.
8. Click **Select Probes** to open the Probe Selector dialog box. It displays a list of available TD140 devices.

9. Select the check boxes for the TD140 devices you want to include in the campaign and click **OK**. You cannot select a TD140 for the campaign if it is disconnected, or part of another current campaign. The TD140s you select appear in the Probe Selection List in the Campaign Details Pane.
10. Verify your selections and click **Save**. A dialog box appears stating that the transfer will start immediately and asks you whether you want to continue.
11. Click **Yes** to confirm. The Iris server starts the transfer process.

After package transfer is complete, the package(s) will be activated at the scheduled time. After activation, the TD140(s) reboot. It may take up to 5 minutes before the TD140(s) restart. Campaign and TD140 status will update to show success or failure. Monitor TD140 status in the Campaign Details Pane; monitor campaign status in the Campaigns Pane.

Upgrading G10 Probe and Array Firmware

PRIOR TO UPGRADING, YOU MUST READ ALL RELEASE NOTES AND UPGRADE CHECKLISTS TO ENSURE YOU ARE AWARE AND COMPLIANT WITH THE LATEST UPDATES TO THE UPGRADE PROCESS. FAILURE TO COMPLY WITH THE LATEST UPDATES COULD PROLONG THE PROBE UPGRADE PROCESS AND RESULT IN EXTENDED DOWN TIME. CONTACT CUSTOMER SUPPORT FOR ASSISTANCE.

Upgrading firmware using the Firmware GUI and campaigns only allows you to upgrade firmware to the available releases shown in the By Probe Firmware tab or Firmware Audit tab. If you need to downgrade firmware for any reason, you need to perform this procedure manually; contact Customer Support for assistance.

You can perform G10 probe and storage array firmware audits and upgrades using the Software tab. Platform packages installed on the G10 probes contain all firmware versions compatible with that platform version. Firmware can be updated for the following components:

- Shmms
- IAP200 (IAP100 NOT included)
- IIC100 boards/AMCs
- IIC200 boards/AMCs
- RAID controller enclosure
- JBOD enclosure

Prerequisites

- The Firmware Administration privilege is required to access Firmware GUIs and campaigns.
- Probes require a minimum of 13.1 software to support this feature.

To View and Export Firmware Inventory for an Individual Probe

1. Click the Software tab.
2. On the By Probe tab, select a probe in the Probe List.
3. Click the Firmware tab to view the inventory for the selected probe. It can take several minutes to initially display.

Upgrades can fail intermittently causing the firmware listing to be incorrect. Click the Refresh Listing button on the Firmware tab to ensure the latest firmware information is displayed in the listing. This can take several minutes to complete.

4. Click the **Export to CSV** button and save the file to a directory on the Iris server. The file is named using **fw_list_ YYYYMMDD_HHMMSS.csv** format.

To View and Export Firmware Inventory for Multiple Probes

1. Click the Software tab.
2. Click the Firmware Audit tab. It can take several minutes to initially display. As a default, inventory for all probes is listed.
3. Click the ellipses (...) button to open the Probe Selector dialog box, and select specific probes or probe groups you want to view firmware inventory.
   - Selecting a group selects all probes in the group.
   - Selecting a TD140 selects all probes bound to the TD140.

- You can view inventory for disconnected probes.

4. Click the **Export to CSV** button and save the file to a directory on the Iris server. The file is named using **fw_list_ YYYYMMDD_HHMMSS.csv** format.

To Determine Probes and Components Requiring Upgrade

Compare the Active and Recommended columns of the exported data to determine the probe components you want to upgrade.

Once you determine which probes require firmware upgrades, verify the Active version listed for these components is also listed as one of the Available versions for that component. If the Active version IS NOT listed in the Available versions, it could indicate that a component has a later version of firmware than what is available from the upgrade campaign. DO NOT upgrade the component and contact Customer Support.

To Create a Firmware Upgrade Campaign

Follow these steps to create a campaign for upgrading firmware on one or more G10s.

1. Click the Software tab, and then click the Probe Campaigns tab. The Campaigns pane appears.
2. Click **Add Campaign**; the Campaign Details Pane appears.
3. Select **Firmware** from the Campaign Type drop-down menu.
4. Enter a name for the campaign.
5. Click **Select Probes** to open the Probe Selector dialog box and select from a list of available probes.
6. Select the check boxes for the probes you want to include in the campaign and click **OK**. You cannot select a probe for the campaign if it is disconnected, or part of another current campaign. The probes you select appear in the Probe Selection List in the Campaign Details Pane.
7. Click the ellipsis **(...)** button to open the Select Devices dialog box which contains all devices configured on the selected probes. If a selected group of probes has dissimilar hardware, the list contains all devices for every selected probe. When you later save the campaign, a Save Report indicates which devices are not applicable to certain probes.
8. Select a date and time to activate the software package. Tektronix Communications recommends scheduling activation during non-peak hours. The G10s require a reboot after activation and this process can take up to 10 minutes.
9. Verify your selections and click **Save**. A Save Report appears and lists which devices are not applicable to certain probes. The issues reported are informational and are not considered errors.
10. Click **OK** to close the Save report. The package(s) will be activated at the scheduled time. After activation, the probes reboot. It may take up to 10 minutes for applications to shut down before the TD140(s) restart. Campaign and TD140 status will update to show success or failure.
11. Monitor probe status in the Campaign Details Pane; monitor campaign status in the Campaigns Pane.

Chapter 7 XDR Profile Management

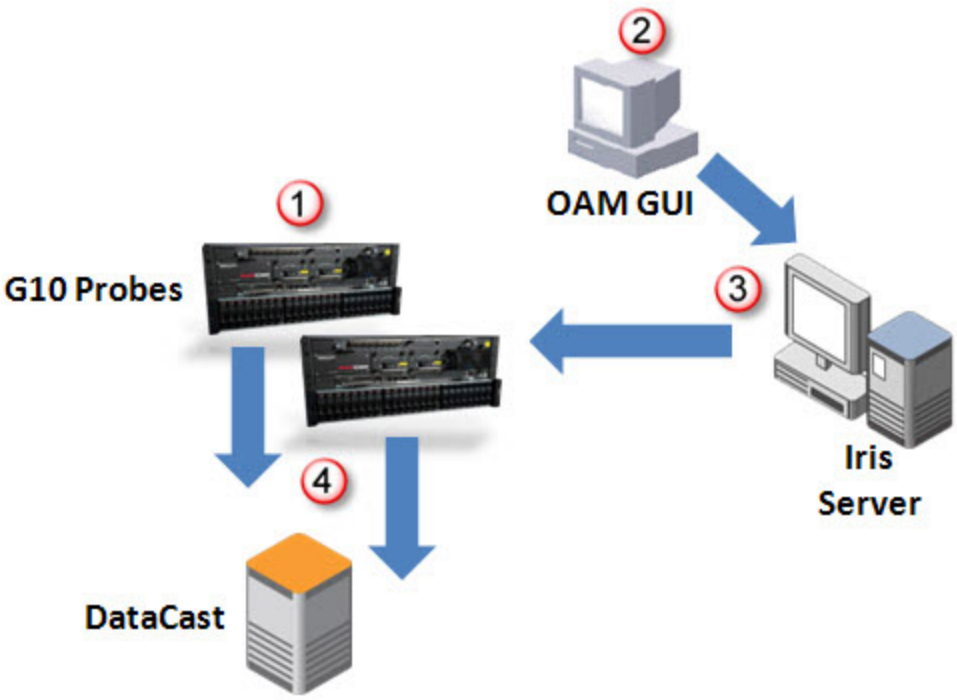
The XDR Profile Management feature on the Applications Tab enables administrators to create protocol-specific profiles to customize G10 data record (XDR) generation. XDRs can be forwarded to the DataCast mediation platform.

Refer to the following sections for more information:

- XDR Generation Process
- XDR Profile Configuration Workflow
- Supported XDR Profiles

XDR Generation Process

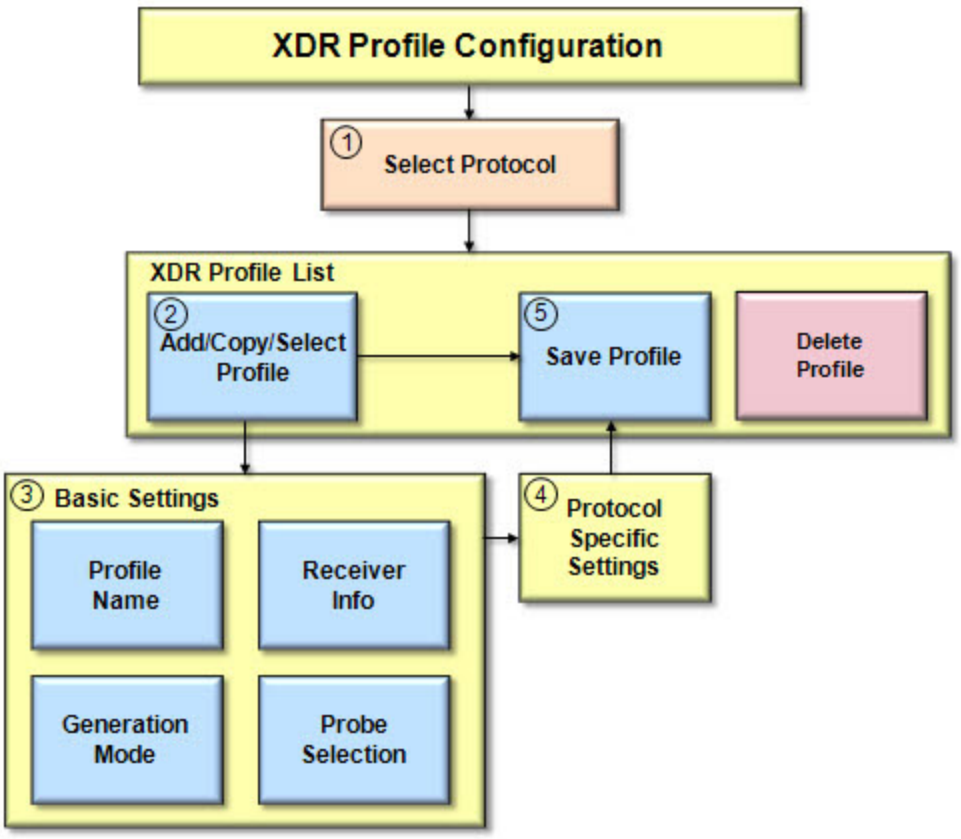
The following graphic summarizes the XDR generation process.



1	**Probes collect data in real time, 24 hours a day, 7 days a week.**
2	**The System Administrator creates and saves XDR profiles on the Admin GUI.**
3	**The Profile is saved to the Iris Server and sent to G10 probes.**
4	**Once a monitored session meets defined profile criteria, the probe generates one or more XDRs and streams them to the defined receiver (DataCast).** • Probes support dynamic profile updates. When the Admin enables a profile for a session already in progress, the entire session is recorded in the XDR.

XDR Profile Configuration Workflow

You configure XDR profiles on the Traffic Tab accessed from the Applications Tab. You create protocol-specific profiles to customize G10 data record (XDR) generation. XDRs can be forwarded to the DataCast mediation platform.



1. Select a protocol. Existing profiles for that protocol appear in the XDR Profile List pane.
2. Perform one of the following tasks:
   - Add a new profile.
   - Copy an existing profile.
   - Select an existing profile.

   The Basic Settings Tab appears blank for new profiles, or displays details for existing profiles.
3. Define basic profile settings on the Basic Settings Tab, including generation mode, receiver IP address/ port and G10 probes.
4. Define protocol-specific settings. Only select protocols provide these additional settings.
5. Save the profile.

Supported XDR Profiles

The following table provides details for supported XDR profiles. See the XDR Profile Configuration Workflow for configuration details.

The "Change" generation mode option only applies to GTP and is only used for GTP Split Monitoring. See Configuring XDRs for GTP Split Monitoring Use Case for details.

Protocol	Available Generation Modes	Recommended Generation Mode	Protocol Specific Settings	Notes
A11	Closure Periodic	Periodic	HTTP Parameters	
ANSI ISUP	Closure Periodic	Closure	Not applicable	
CNAM	Closure Periodic	Closure	Not applicable	
DHCP	Closure Periodic	Closure	Not applicable	
DIAMETER	Closure Periodic	Closure	Not applicable	
DNS	Closure	Closure	Not applicable	
DSS1	Closure Periodic	Closure	Not applicable	
GTP	Change Periodic	Periodic	HTTP Parameters	The HTTP parameters in this profile are not used for probes supporting GTP Split Monitoring. See Configuring XDRs for GTP Split Monitoring Use Case for details.
GTPv2	Change Periodic	Periodic	HTTP Parameters	
H248	Closure Periodic	Closure	Not applicable	
H323CS	Closure Periodic	Closure	Not applicable	
ISAIC	Closure Periodic	Closure	Not applicable	
ITU ISUP	Closure Periodic	Closure	Not applicable	
LDAP	Closure	Closure	Not applicable	
LNP	Change Closure Periodic	Closure	Not applicable	

Protocol	Available Generation Modes	Recommended Generation Mode	Protocol Specific Settings	Notes
LTE-RRC	Closure Periodic	Closure	Not applicable	This protocol is only supported by the GeoSoft RAN probe.
MGCP	Closure Periodic	Closure	Not applicable	
PMIPv6	Closure Periodic	Periodic	Not applicable	
RADIUS	Closure Periodic	Closure	Not applicable	
RTP+RTCP	Closure Periodic	Periodic	Not applicable	
RTSP	Closure Periodic	Periodic	Not applicable	
S1AP	Closure Periodic	Periodic	Not applicable	
SGsAP	Closure Periodic	Periodic	Not applicable	
SIP	Closure Periodic	Periodic	SIP Parameters	
TOLLFREE	Closure Periodic	Closure	Not applicable	
User Plane	This option is only used for probes supporting GTP Split Monitoring Architecture. Specific XDR profiles are required to support GTP Split Monitoring; see Configuring XDRs for GTP Split Monitoring Use Case for details.			
XCAP	Closure Periodic	Periodic	HTTP Parameters	

Chapter 8 Iris Maps Configuration and Administration

This chapter provides a workflow for the configuration required for enabling users to view Iris and GeoProbe elements on their Iris Network Maps.

Iris Maps Configuration Workflow

Prerequisites

- Allocate the ports required for Iris Network Maps (see Iris System Requirements).
- Tektronix installs Network Maps application and map backgrounds provided by the Geographic Information System (GIS) framework.
  - Tektronix determines appropriate map packages including zoom level layers to support your network coverage.
  - The Maps application requires no configuration by the administrator for map background selection.
- Tektronix defines network connectivity between the GeoProbe server and the Iris server (see Servers Tab for details).
  - All nodes, linksets, and interfaces associated with the GeoProbe map are automatically visible.
  - Each map defined in GeoProbe is a separate layer in Iris Maps.
  - Changes in GeoProbe-configured nodes or linksets are automatically reflected in Iris Maps without intervention from the user or the administrator. Refer to the GeoProbe documentation for more details about GeoProbe system configuration.

To Configure Iris Network Maps

1. Define default longitude and latitude values and mapping rules for placement of GeoProbe and Iris probes and nodes on maps (see Locations Tab).
2. If necessary, adjust Iris individual node or probe locations manually; for example, if you want to separate node clusters resulting from rules-based node placement. See the Node Details Pane and the Probe Details Tab.

   Once manually assigned, coordinates are not overwritten by mapping rules. GeoProbe node and probe geocodes can only be managed by defining rules in the Locations Tab.
3. Define Iris map layers for Iris elements by defining node and probe groups (see Groups Tab for details).
   - Each defined Iris node and probe group is a separate layer in the map that can be shown or hidden.
   - Iris Maps is installed with a default All Probes group which cannot be modified or deleted.
4. Within UUMS, assign maps users roles with relevant user privileges for maps access and functions (see UUMS online help for details).

Appendix A

Admin User Interface

Applications Tab	• Applications Tab • Store to Disk Tab • Traffic Tab • RIF Profile Tab • ITA Configuration Tab • ISA Configuration Tab • IFC Configuration Tab • Persistent Capture Tab
Licenses Tab	• Licenses Tab
Probes Tab	• Probes Tab • Probe Details Tab • Timing Control Tab • Monitoring Details Tab • Media Configuration Tab • ISA Configuration Tab • Storage Maintenance Tab • TD140 Ports Tab • TD140 Details Tab • TD140 Managed Probe Tab
Software Tab	• Software Tab • By Probe Tab • Available Patches Tab • Campaign Details Pane • Campaigns Pane • Probe Campaigns Tab
System Tab	• Servers Tab • Config Import Tab • Config Export Tab

Topology Tab	• Topology Tab • Managed Objects Tab • Entities Pane • Application Details Pane • Physical Link Details Pane • Logical Link Details Pane • Protocol Details Pane • Node Details Pane • Audit Log Dialog Box • Groups Tab • Auto Detection Tab • Add Group Members Dialog Box
Locations Tab	• Locations Tab

Applications User Interface

Admin contains the following Applications GUI elements.

- Applications Tab
- Store to Disk Tab
- Traffic Tab
- RIF Profile Tab
- XDR Profile List Pane
- Basic Settings Tab
- Protocol Specific Tab
- ITA Configuration Tab
- ISA Configuration Tab
- IFC Configuration Tab
- Persistent Capture Tab

Applications Tab

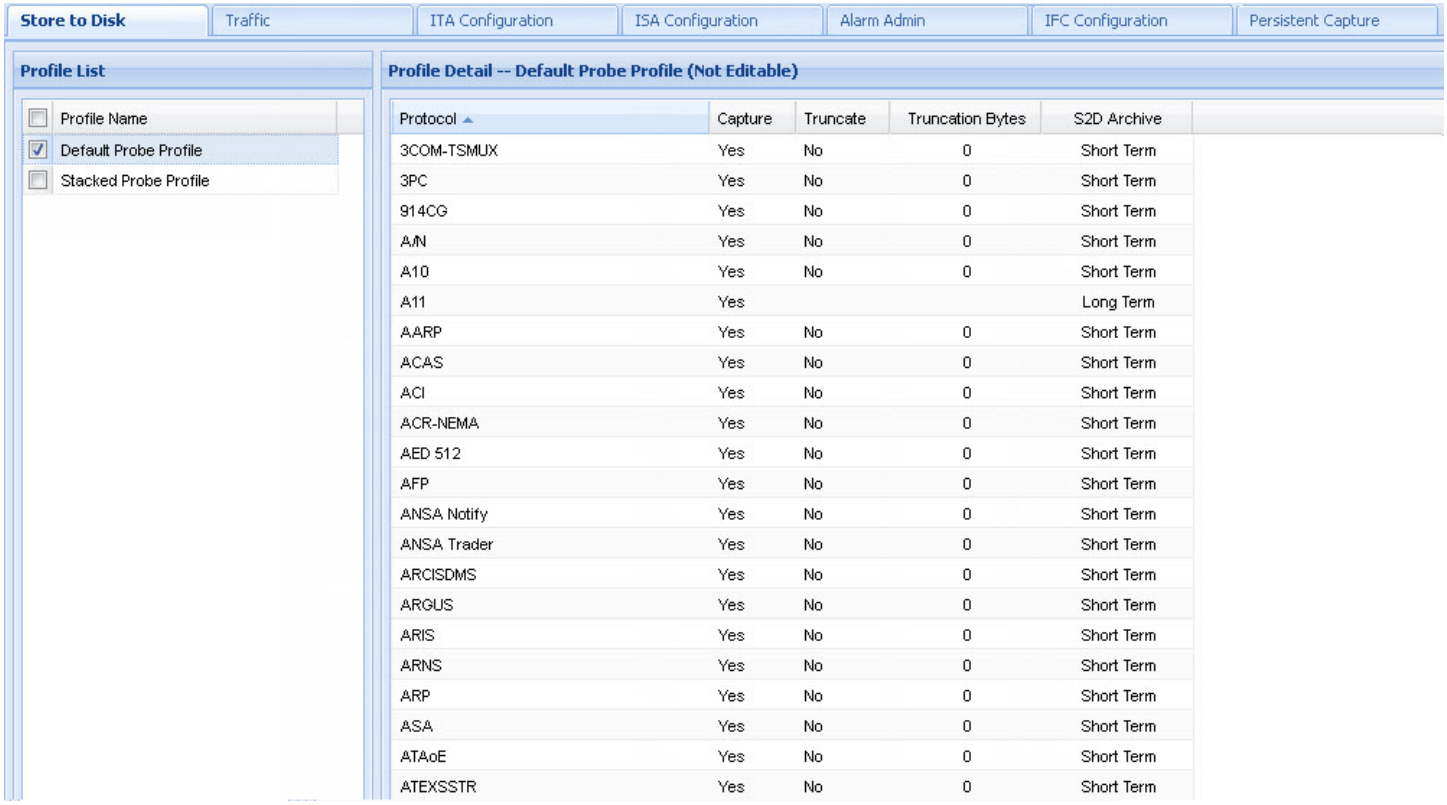
The Applications tab enables you to manage configuration settings for Store to Disk, ISA, ITA, XDR, and IFC Profile Management.

Applications Tabs

Store to Disk Tab	Manage which protocol PDU data is stored to long-term or short-term archives on the storage arrays.
Traffic Tab	Manage protocol-specific profiles for G10 XDR generation.
RIF Profile Tab	Manage RAN Intelligence Feed configuration for 3G GeoSoft RAN Probes.

ITA Configuration Tab	Set system defaults to control ITA dashlet display.
ISA Configuration Tab	Set a system default to control the order in which node types display in the ISA Ladder Diagram.
IFC Configuration Tab	Set profiles to schedule sessions for later retrieval from the local disk or a remote server repository.
Persistent Capture Tab	Set profiles to schedule long-running session traces of user plane data by IMSI or MSISDN.

Applications Tab



Store To Disk Tab

The Store to Disk feature enables you to manage which protocol PDU data is stored to long-term or short-term archives on the storage arrays. The default probe profile and new profiles have the following default settings:

- Capture and store all protocol PDUs to storage array
- Store control plane protocol data supported in ISA in long-term volumes
- Store user plane protocol data and control plane data not supported in ISA in short-term volumes
- Do not truncate packets for any protocol

You can use the default probe profile or create customized profiles. Profiles are assigned to individual probes on the Probes tab. See Managing Iris Data Storage for details about creating customized profiles.

Profile List Pane

Create, delete, or copy S2D profiles.

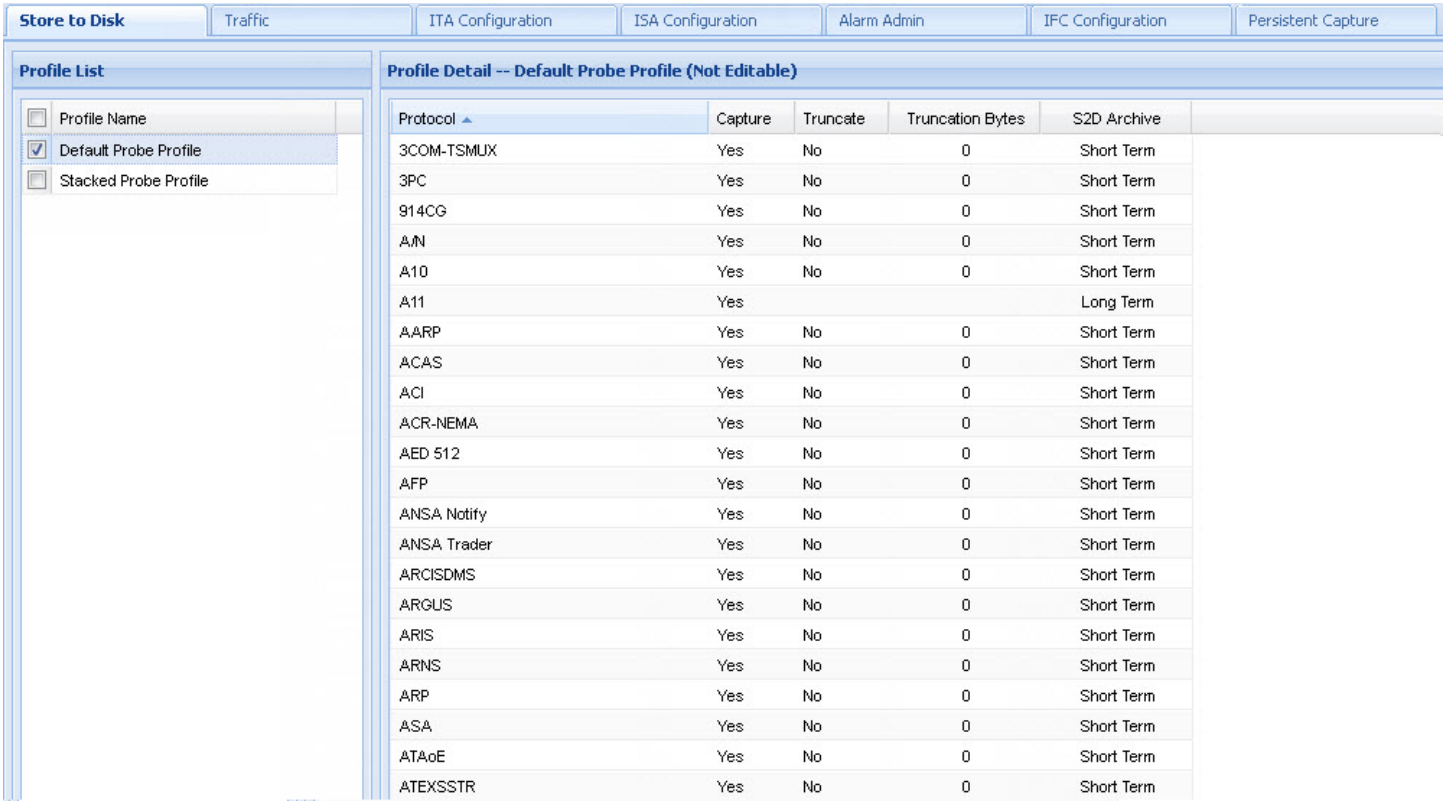
Profile Name Check Box	Select the top check box to select all check boxes in the column. You can also select individual profiles and then click the Delete or Copy buttons, as needed.
Profile Name List	You cannot edit the Default Probe Profile, Stacked RTP Profile, or Stacked Control Plane Profile.
New Button	Open the Create a New Profile dialog box and enter a name for the new profile. Click Create button to add the new profile to the list.
Delete Button	Delete one or more profiles you have selected in the profile name check boxes.
Copy Button	Open the Copy Profile to dialog box and enter a name for the copied profile. Click the Copy button to add the copied profile to the list.

Profile Detail Pane

Configure capture details for each protocol type.

Protocol Column	Lists the names of supported protocols and those you create in the Protocol Details Pane of the Managed Objects tab.
Capture Check Boxes	Indicates if you want to capture and store to disk packets for the corresponding protocol (application). All protocols are enabled by default.
Truncate Check Boxes	Indicates if you want to truncate the packet for this protocol. By default, no packets are truncated. If you check this box, you must also enter a value for the number of bytes you want to save to disk after truncation (4095 bytes maximum), counting from the header down.
Truncation Bytes	*HTTP truncation can only be enabled or disabled; you cannot control the amount of HTTP payload that is truncated. The G10 truncates HTTP packets as defined in IP Packet Truncation. You disable HTTP truncation by setting the Truncate Bytes field to 0; you enable HTTP truncation by setting this field to 1.*
S2D Archive Column	Indicates whether the data associated with a specific protocol should be saved to a short term or long term archive on the storage array. Click the corresponding cell in this column to edit the setting.
Save Profile Button	Save the changes. • If creating new profiles, the profile can now be assigned to individual probes in the Probe Tab. See Configuring G10 Probes for more information. • If modifying existing profiles, the changes are immediately uploaded to the probes that are assigned this profile.

Store to Disk Tab

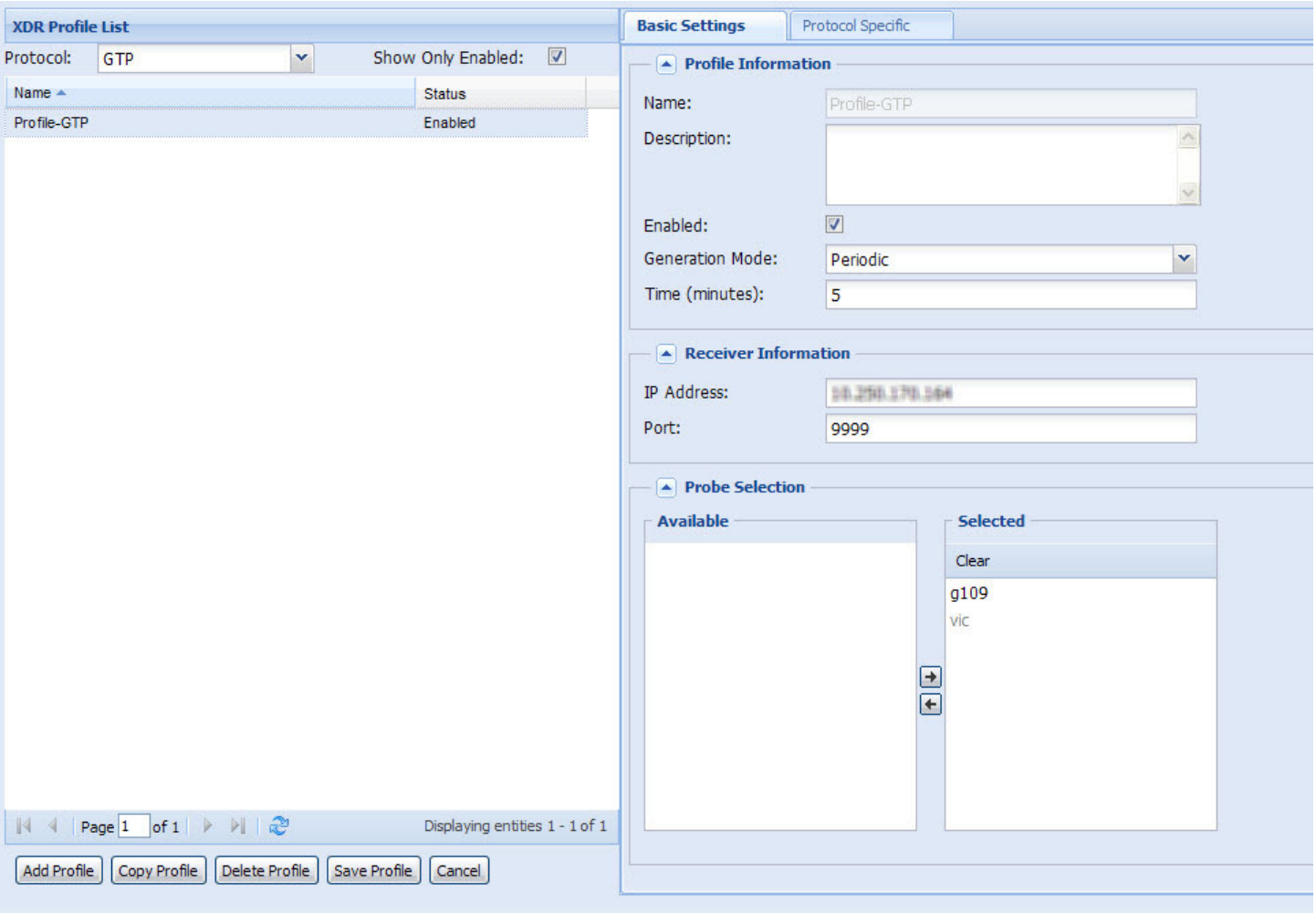


Traffic Tab

The Traffic tab enables you to manage protocol-specific profiles for G10 XDR generation. See XDR Profile Configuration Workflow for details.

XDR Profile List Pane	View a list of all defined profiles for a selected protocol. Add, copy, delete, or save profiles from this pane.
Basic Settings Tab	Configure profile details such as name and generation mode, receiver information, and probe selection.
Protocol Specific Tab	Only accessible for select protocols (see Supported XDR Profiles for details). Currently this tab supports: • HTTP Parameters • SIP Parameters

Traffic Tab



XDR Profile List Pane

The XDR Profile List pane enables you to view a list of all defined profiles for a selected protocol. You can add, copy, delete, or save profiles using this pane. You must first select a protocol to view associated profiles.

Pane Controls

Protocol Drop-Down Menu	Select a protocol to view a list of existing XDR profiles. Iris does not provide default XDR profiles. If no profiles have been defined, this area is empty.
Show Only Enabled Check Box	Select this check box to display, in the XDR Profile List, those profiles that were enabled in the Basic Settings Tab.
Add Profile Button	Opens the Basic Settings tab showing blank fields.

Copy Profile Button	Create a copy of the selected profile. • Profile name appears as "Copy_of_" and you can modify it. • Profile details are copied to a new profile • Probe Selection details are **not** copied because same probe cannot be selected in multiple profiles within the same protocol. • Default Status is disabled.
Delete Profile Button	Permanently delete the profile. Changes take effect immediately and XDRs are no longer generated for the deleted profile.
Save Profile Button	Save all profile settings. This button is not enabled until all required fields are populated on all tabs.
Cancel Button	Close the Basic Settings Tab and Protocol Specific Tab without making any changes.

Columns

Name Column	The name of the profile. Select a profile name to view its details in the Basic Settings Tab.
Status Column	Indicates whether the profile is enabled or disabled. You edit this setting in the Basic Settings Tab.

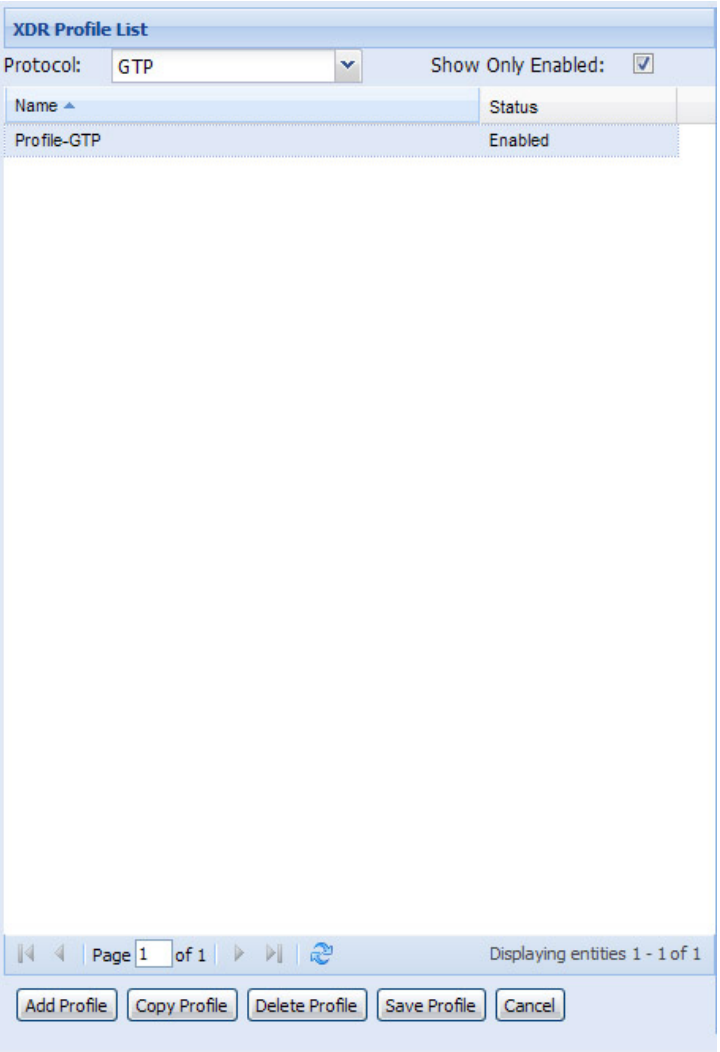
Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the check mark from columns you want to hide. At least one column must remain visible.

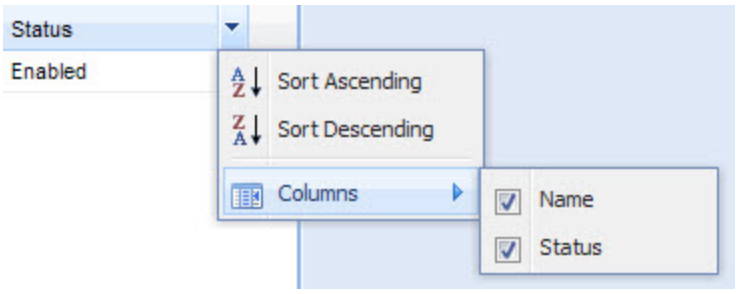
Pagination Controls

Page Field	Enter a page number in the field and click the Next or Previous buttons to display the corresponding page content in the list pane. This enables you to quickly locate a specific page when there is a large number of items.
Next Button	
Previous Button	
Begin/End Buttons	Display the first page or the last page in the list.
Refresh Button	Manually refresh the list.

XDR Profile List Pane



Column Filters

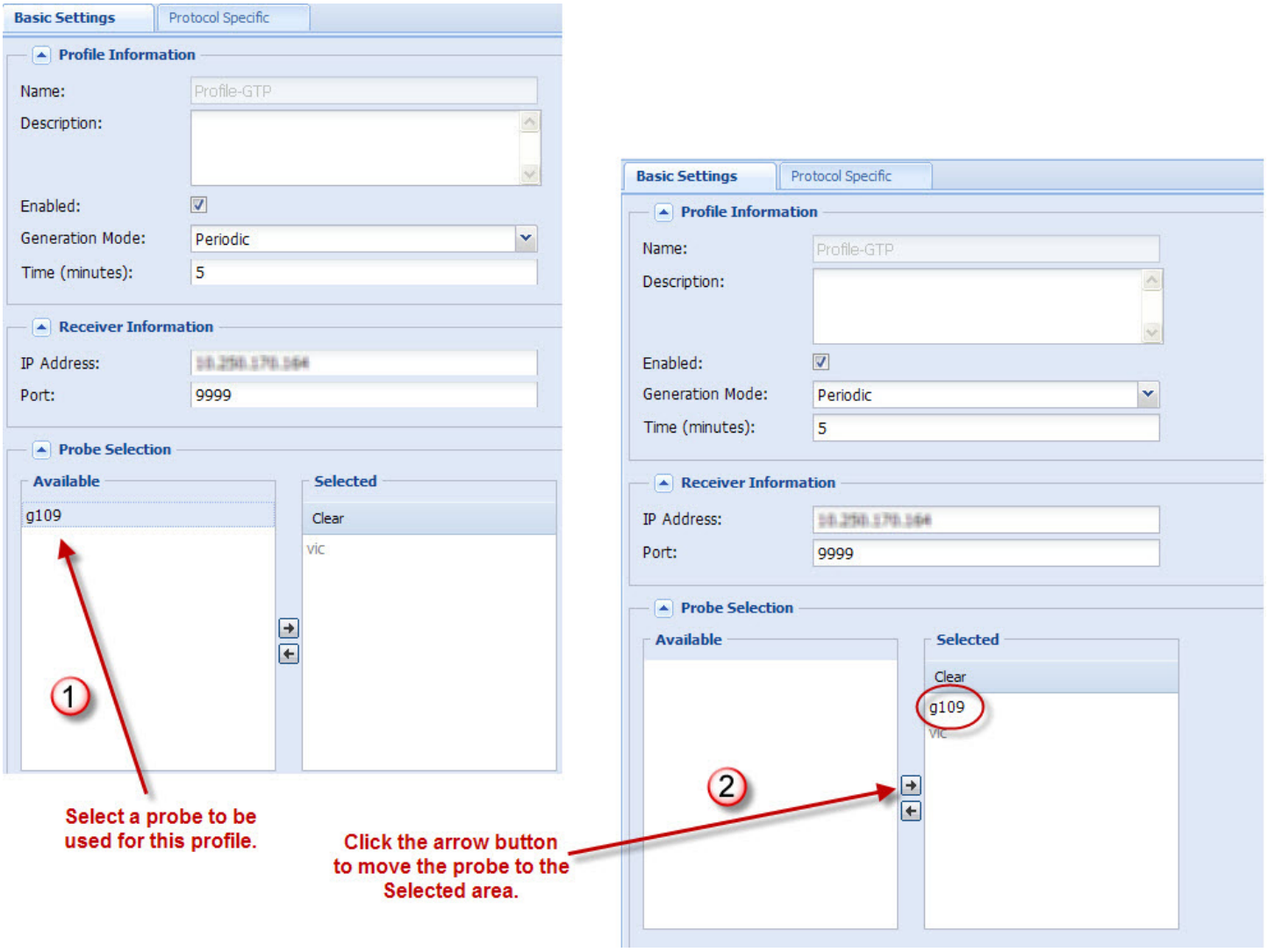


Basic Settings Tab

The Basic Settings Tab enables you to configure profile details such as name and generation mode, receiver information, and probe selection. You access this tab by selecting an existing profile or by clicking the Add Profile button in the XDR Profile List Pane.

Name	Enter a unique name for the profile.
Description	Enter a description for this profile.
Enabled	A checkmark indicates the profile is enabled. This checkbox is enabled by default.
IP Address	Enter the IP address for the DataCast server.
Port	Enter the Port ID on the DataCast server.
Generation Mode	Select a generation mode for the XDR: • Periodic - an XDR is generated at a specific time interval. To select this option, you can select Periodic and then enter the time interval in the Time field. • Change - This option is only used for probes supporting GTP Split Monitoring Architecture. Specific XDR profiles are required to support GTP Split Monitoring; see Configuring XDRs for GTP Split Monitoring Use Case for details. • Closure - a single DR is generated at the end of a session.
Time	Enter the time interval, in minutes, you want the XDR generated. This option is only enabled when you select Periodic Generation mode.
Probe Selection - Available	Displays a list of available probes. This list is made up of probes which are not already in use by any other profile within the selected protocol.
Probe Selection - Selected	Displays the list of selected probes for this profile. Use the arrow keys to move probe names from the Available list to the Selected list.

Basic Settings Tab



Protocol Specific Tab

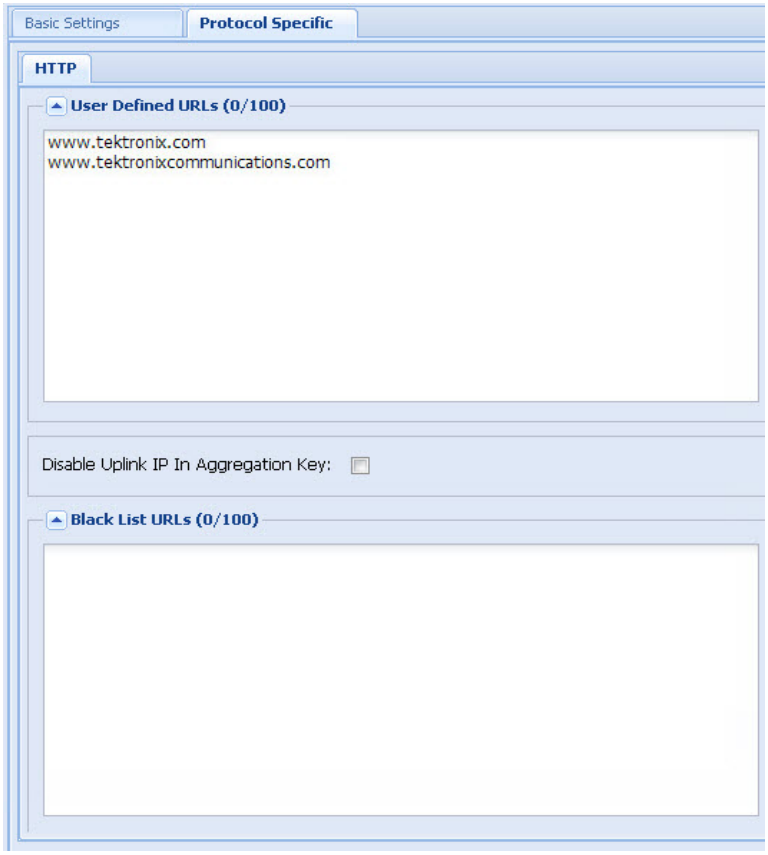
The Protocol Specific Tab is only accessible for select protocols, and the contents of this tab varies per protocol. See Supported XDR Profiles for details about which protocols support this tab.

HTTP Tab

The Protocol Specific tab for HTTP is only accessible for select protocols. This tab enables you to configure up to 100 White List and 100 Black List HTTP URLs for probes to analyze and process for XDRs.

User Defined URLs (White List) (0/100)	Include statistics for each URL in the HTTP session and total aggregated statistics for all URLs in the session. Up to 100 URLs may be entered. If you enter the same URL in the User Defined section and the Black List, the Black List takes precedence on the probe. Supported URL formats are: • http://www.tektronix.com • www.tektronix.com • tektronix.com For a list of statistics that are included in the XDR for each URL, refer to the Iris Performance Intelligence (IPI) GTP-U Performance KPIs; a complete list of these KPIs is provided in the Iris Online Help.
Disable Uplink IP in Aggregation Key Check Box	Select this check box if you want to exclude uplink IP address from the Gi User Plane aggregation key in DRs. Enable this option to calculate URL counts and eliminate anomaly scenarios that can skew data such as when multiple servers support the same URL.
Black List URLs (0/100)	Exclude statistics from the generated XDR for these URLs. If these URLs are seen, they are counted in the total aggregated statistics for "Unknown" URLs in the XDR. Up to 100 URLs may be entered. The Black List 100 URL limit is separate from the White List limit of 100.

HTTP Tab

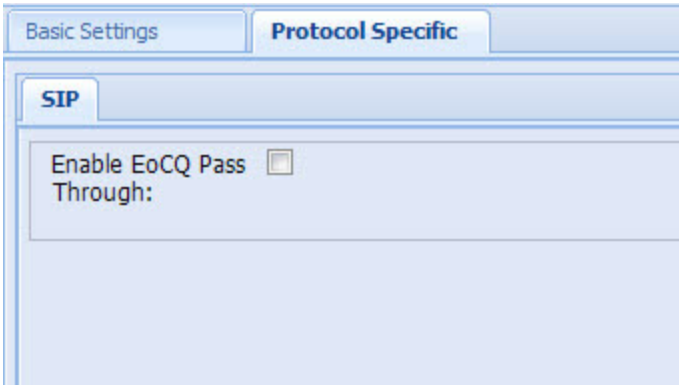


SIP Tab

The Protocol Specific tab for SIP is only accessible for SIP XDRs. This tab enables you to control how SIP Publish EoCQ content is processed during XDR generation. The SIP Publish EoCQ content provides metrics that measure quality for RTP sessions.

Enable EoCQ Pass Through Check Box	• **Disabled (Unchecked):** The G10 probe parses Information Elements (IEs) out of the incoming SIP EoCQ message, and includes them in an XDR. This option supports the Iris applications. • **Enabled (Checked):** The G10 probe includes the full unparsed body of the incoming SIP EoCQ message along with the parsed IEs in one XDR. This option supports the Iris applications as well as other third-party tools that parse the data themselves.

SIP Tab



XDR HTTP URL Longest Match Criteria

Select XDR Profiles allow you to define White List and Black List URLs to either include or exclude from XDRs. You define these HTTP URLs on the Protocol Specific HTTP Tab in the Traffic tab.

White List Matching Criteria

All unique URLs added to the White List URLs list are stored on the probe in a minimally normalized form: lower case with any "http://" prefix and any trailing "/" removed.

The URLs tracked by the probes use a "Longest Match" criteria for matching URLs and placing URL tags in the XDRs. Longest Match is a method that inserts the configured URL in the XDR that has the closest match to the URL seen.

If there is no match, then the URL for the XDR is included in the aggregated total for "Unknown" URLs.

URL Seen in Traffic	Provisioned White List	Result
www.yahoo.com/sports	www.yahoo.com	www.yahoo.com
	www.yah.com	
	www.google.com	
www.yahoo.com/sports	www.yahoo.com	
	www.yahoo.com/sports	www.yahoo.com/sports
	www.google.com	
www.yahoo.com/sports	www.jabber.com	
	www.woot.com	
	www.google.com	
		UNKNOWN
www.yahoo.com/sports	www.yahoo.com/auto	
	www.yahoo.com/finance	
	www.google.com	
		UNKNOWN

Black List Matching Criteria

As with White List URLs, Black List URLs are stored on the probe in a minimally normalized form: lower case with any "http://" prefix and any trailing "/" removed.

The matching algorithm for Black List URLs is an exact match of the normalized URL host. When a probe finds a match in the Black List, it aggregates the URL against the "Unknown" category in the XDR.

URL Seen in Traffic	Black List	User Defined White List	Result
http://bigpond.wz.com.au/images/graphics/ bluefade.jpgHost = bigpond.wz.com.au URI = /images/graphics/bluefade.jpg	bigpond.wz.com.au[1]		Unknown
		bigpond.wz.com.au	
		bigpond.wz.com.au/images/graphics/ bluefade.jpg	
www.google.com/loc/m/api Host = www.google.com URI =/loc/m/api	www.google.com/loc[2]		
		www.google.com	www.google.com

[1]Even though there is a matching URL in the User Defined List, the Black List takes precedence and URL is tagged as "Unknown."

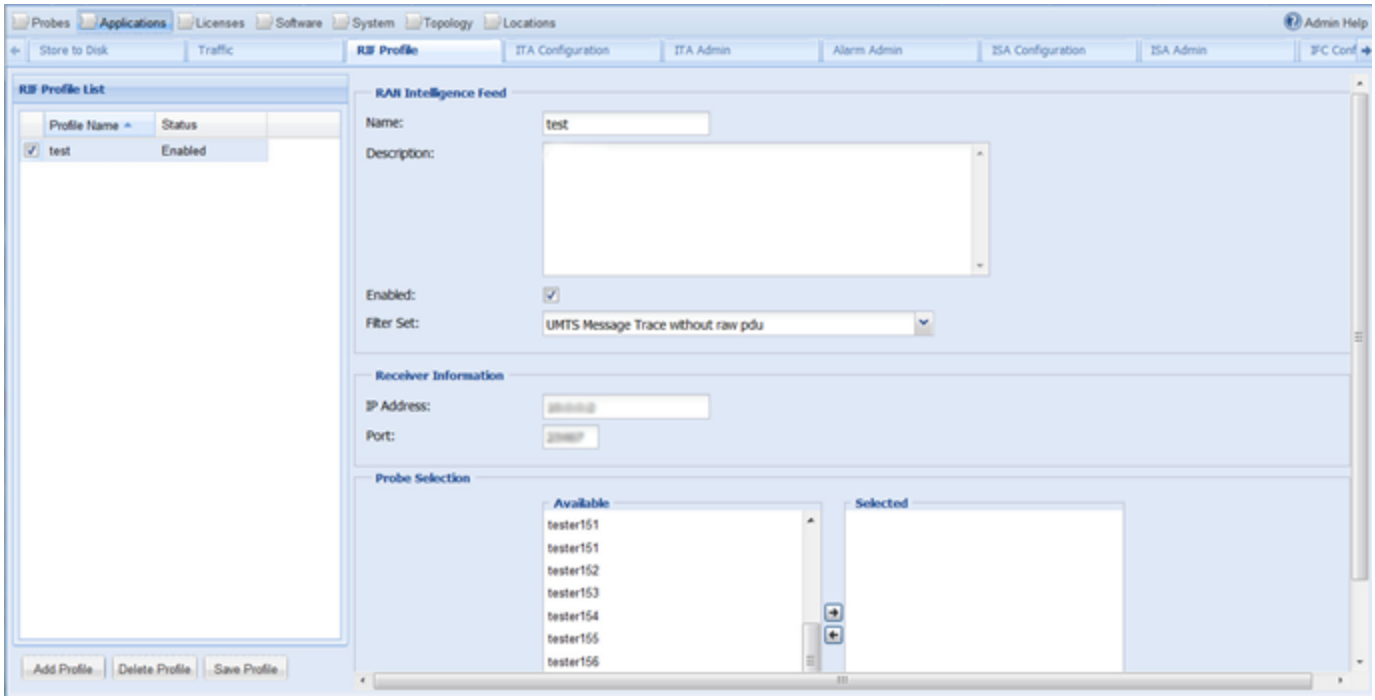
[2]The URL does not match the Black List exactly, so the probe matches the URL to the User Defined White List (www.google.com) and assigns it to that URL category within the XDR.

RIF Profile Tab

GeoSoft RAN 3G probes provide a RAN Intelligence Feed for geolocation analysis. This enhanced xDR feed includes RAN statistics and measurement reports required for RAN optimization use cases.

RAN Intelligence Feed is the name for a data feed provided to 3rd party applications with the focus on geolocation processing which is based on RAN signaling data. GeoSoft RAN probes will create records that contain the necessary data to achieve this task. These records are typically sent to the xDR receiver server where they can be filtered and sent to one or more registered client applications. The probe feature to generate RIF data is controlled by profiles managed in IRIS OAM.

The RIF Profile tab enables you to manage configure RAN Intelligence Feeds:



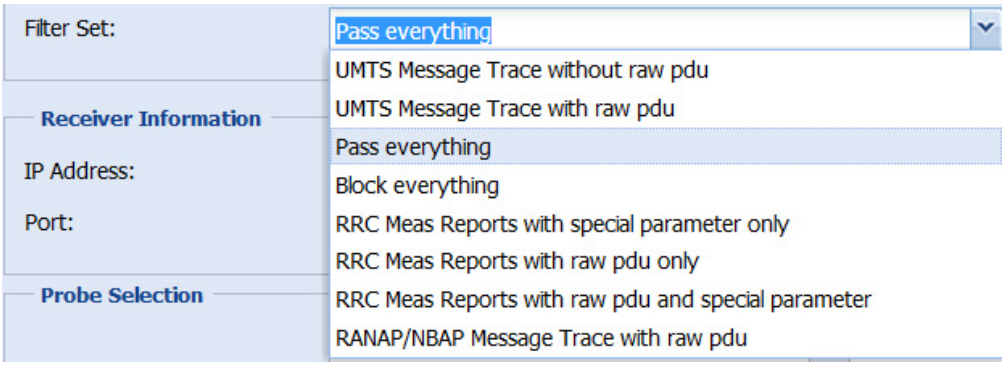
The **RIF Profile List** pane enables you to view a list of all defined profiles for a selected protocol. You can add, delete, or save profiles using this pane. You must first select a protocol to view associated profiles.

RIF Profile List Pane

Enabled Column Check Box	Select this check box to select a RIF Profile in the RIF Profile List.
Profile Name Drop-Down Menu	Displays the profile names of the existing RIF profiles. Iris does not provide default profiles. If no profiles have been defined, this area is empty.
Status	Displays the status of the existing RIF profiles.
Add Profile Button	Opens blank fields in the RAN Intelligence Feed.
Delete Profile Button	Permanently delete the profile. Changes take effect immediately and RIFs are no longer generated for the deleted profile.
Save Profile Button	Save all profile settings. This button is not enabled until all required fields are populated on all tabs.

RAN Intelligence Feed Pane

Name	Enter a unique name for the profile.
Description	Enter a description for this profile.
Enabled	A check mark indicates the profile is enabled. This checkbox is enabled by default.

Filter Set:	Select the filters for the RIF function from the predefined Filter Set drop down list. 

Receiver Information Pane

IP Address	Enter the IP address for the xDR receiver server (e.g. of the Datacast server) .
Port	Enter the Port ID of the xDR receiver server (e.g. of the Datacast server) .

Probe Selection Pane

Probe Selection - Available	Displays a list of available probes. This list is made up of probes which are not already in use by any other profile within the selected protocol.
Probe Selection - Selected	Displays the list of selected probes for this profile. Use the arrow keys to move probe names from the Available list to the Selected list.

ITA Configuration Tab

The ITA Configuration Tab enables you to set system-wide defaults for ITA dashlets.

Nodes by Volume Config Area

Top N Value Field	Specify how many highest volume nodes the Nodes by Volume dashlet displays by default. The maximum is 25.

Dashlet by Direction Area

Display Option	Set the system default to one of the following options: • Inverted - Display minimum-to-maximum graph data from top to bottom. This option affects only the downlink part of the dashlet. • Standard - Display minimum-to-maximum graph data from bottom to top. See Standard vs. Inverted Display Example.

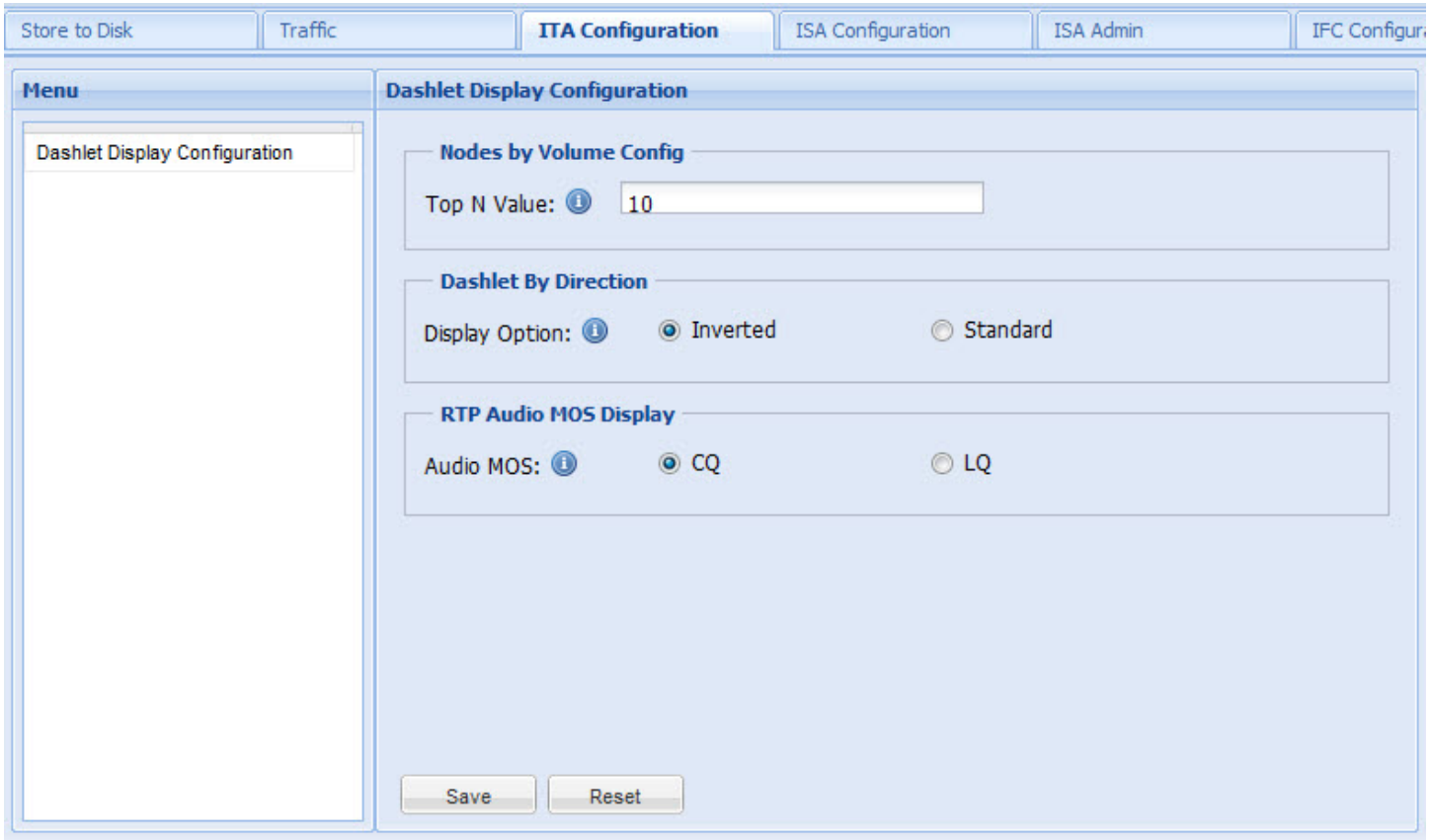
RTP Audio MOS Display

Audio MOS	Set the system default to one of the following options: • CQ - Display Conversational Quality MOS • LQ - Display Listening Quality MOS

Controls

Save Button	Save your changes and apply them as the default. The new settings only apply to new users created after the defaults are modified. Users can override the default settings by changing their Preferences from the ITA Dashboard. Refer to the Iris Online Help for details.
Reset Button	Click the Reset button to revert back to the Tektronix Communications system defaults.

ITA Configuration Tab



Standard vs. Inverted Display Example

Inverted Display

Standard Display

ISA Configuration Tab

The ISA Configuration tab enables you to define mount points for IFC profiles, define ISA failure transactions and ISA and ITA timeout and failed classifications, and set a system default to control the order in which node types display in the ISA Ladder Diagram. See Configuring ISA Default Node Type Order for details.

Menu Area

Global Probe Configuration	Contact Tektronix Communications Customer Support.
System Default Node Type Order	Specify the default order in which node types appear in the Ladder Diagram for ISA users.
IFC Mount Points	Define network file system mount points to which IFC profiles export session records from scheduled searches. The mount points defined in this area appear in an options menu that becomes available when you select the Disk export option in the IFC Profile Configuration window.
Failure Configuration	For G10 probes, define the transactions that appear as failure and timeout transactions in ISA and ITA. If you select the Timed Out option in the Failed Transaction Configuration area, the timeout is applied to its failure KPI. To enable separate Timeout KPIs, do not select this option.
Indicator Configuration	Define the failed and timeout classifications in ISA for network applications by probe type.

System Default Node Type Order

Use these buttons to adjust the order of node type display in the ISA Ladder Diagram. The first node type in the list appears at the leftmost position in the Ladder Diagram for applicable sessions and the remaining node types in the list appear to the right as listed.

Available Node Types	Lists all available G10 and SpIprobe monitored node types. You can select from this list any node types that you want to appear in a certain order in the ladder and move them to the Selected list.

UNKNOWN Node Type	The UNKNOWN node type is used as a wildcard. You can assign it to the Selected list in place of all node types not included in the list. Node types that have not been assigned any order will appear together in the Ladder Diagram in place of the UNKNOWN node type in time-based order.
Selected Node Types	Shows the order in which the node types appear in the Ladder Diagram. The list initially contains a Tektronix Communications-defined system default order for the node types based on typical call flows.
	• Select a node type from the Selected list and click the **Move to Top** button to move it to the top of the list. This node type will be the leftmost node type shown in the ISA ladder diagram for applicable sessions. • Select a node type from the Selected list and click the **Move to Bottom** button. This node type will be the last node type shown at the right in the ISA ladder diagram for applicable sessions.
	• Select one or more items from the Selected list and click the **Move Up** or **Move Down** buttons to move the items one position at a time in the list. • Use the CTRL and SHIFT keys to select multiple items.
	• Select one or more items from the Available list of node types and click the right arrow button to move them to the Selected list. • Select one or more items from the Selected list and click the left arrow button to remove them from the list. • Use the CTRL and SHIFT keys to select multiple items.
Clear Button	Move all nodes from the Selected list to the Available list.
Save Button	Save the settings in the Selected list as the new system default value. All users who select the Custom Order setting in the ISA Ladder Diagram will view the Ladder Diagram with the default node type order. Any modifications you make to the default do not take effect until ISA is restarted or the user changes the system default order in the ISA Results window.
Cancel Button	Cancel changes and revert to the previously saved node type order in the Selected list.

IFC Mount Points Configuration

Add new mount points for IFC profiles.

Mount Points Area	• Add a new mount point by clicking the New button. • Edit a mount point by selecting it and clicking the Edit button, or double-click the mount point entry. • Delete a mount point by selecting it and clicking the Delete button. • Save a mount point by clicking the Save button. The new mount point becomes available for selection in the IFC Profile Configuration window. • Reset the IFC Mount Points Configuration area. You will lose any unsaved changes.

Failure Configuration

For G10 probes, define failed responses for transactions and failed transactions per protocol. The Failure Configuration options only affect future records.

Failed Response Configuration Area	• Select a protocol from the Protocols area. • Select a combination of protocol/transaction type/response codes. Your choices vary depending on the protocol you select. • Select a combination of protocol/transaction/message type. Your choices vary depending on the protocol you select.
Failed Transaction Configuration Area	• Select the transaction status to assign to the transaction: Retransmission, Timed Out, Sequence Error, Failed Response, or Incomplete. • To display Timeout KPIs separately in ITA, do not select the Timed Out option. • The Failed Response transaction status option does not affect ISA protocols that have no transaction types: IMAP, MMS,POP3, SMTP, and WSP. • Some protocols are not supported by ISA but are supported by other applications such as ITA. If you select one of these protocols, the following message appears beside Protocols options menu: "This protocol is not supported in session tracking."
Remove Selection Button	• Remove the selected row.
New	• Add a new row.

Indicator Configuration

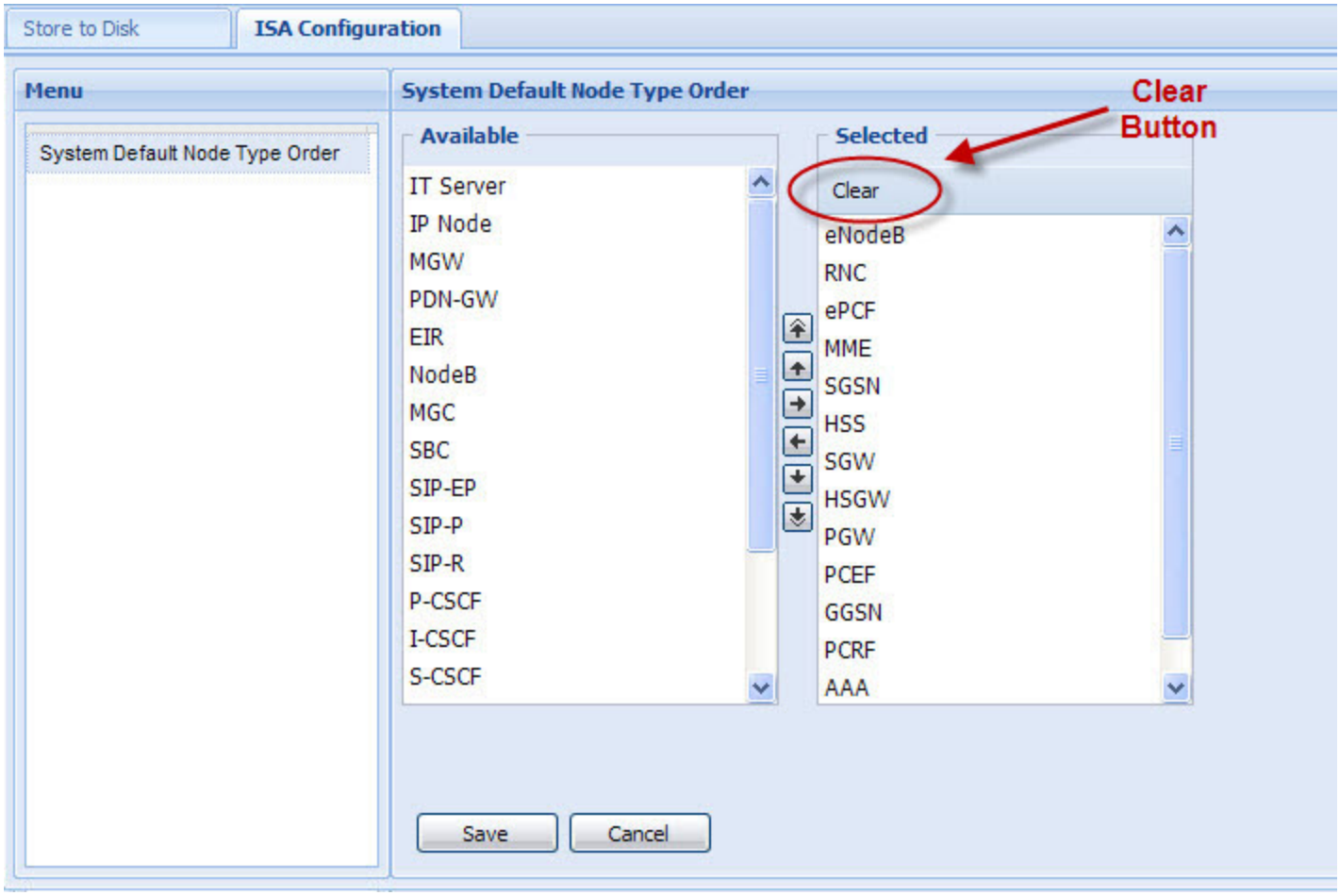
For G10 probes and SpIprobes, define the timeout and failed classification per application. Only ISA sessions started after you save the Indicator Configuration will be affected by the configuration changes.

Failure/Timeout Indicator Configuration	• Select a probe type: G10, SPI, or ALL. • Select a network application type, which might be a protocol or interface. • Select an indicator: Failed, Normal, or Timed Out. • Select the transaction status: Failed or Timed Out. **Configuration priority** For the Probe Type and Application Type, The “ALL” wildcard (*) is supported, so some configurations might conflict. The following list shows the configuration priority from highest (1) to lowest (4): 1. Specified Probe Type + Specified Application Type 2. Specified Probe Type + ALL Application Type 3. ALL Probe Type + Specified Application Type 4. ALL Probe Type + ALL Application **Status priority** In some situations, you might configure the same status to a different Indicator. The following list shows the Indicator priority from highest (1) to lowest (3): 1. Failed indicator 2. Timed Out indicator 3. Normal indicator
Remove Selection Button	• Remove the selected row.

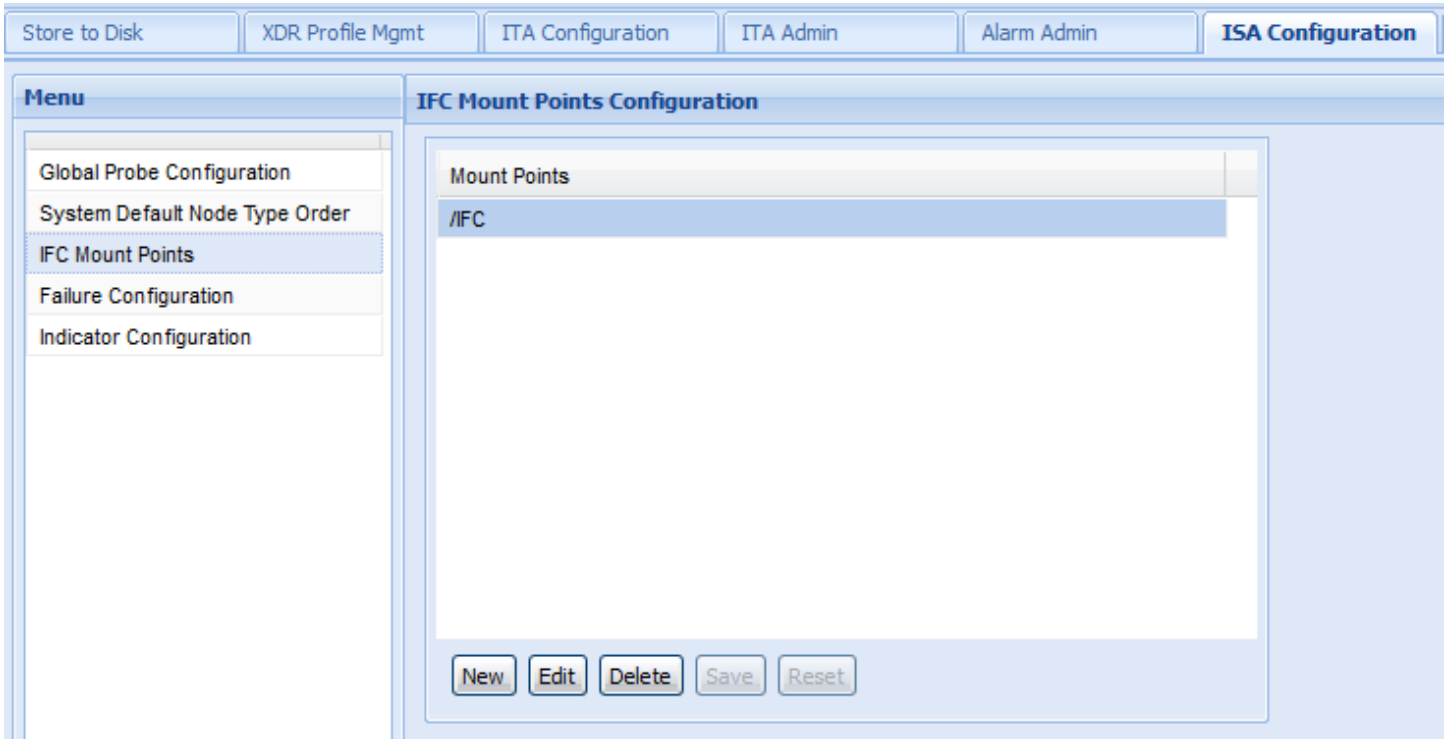
Failure and Indicator Configuration Common Controls

Remove Selection Button	• Remove the selected row.
New	• Add a new row.
Save	• Save your changes.
Cancel	• Cancel your changes.

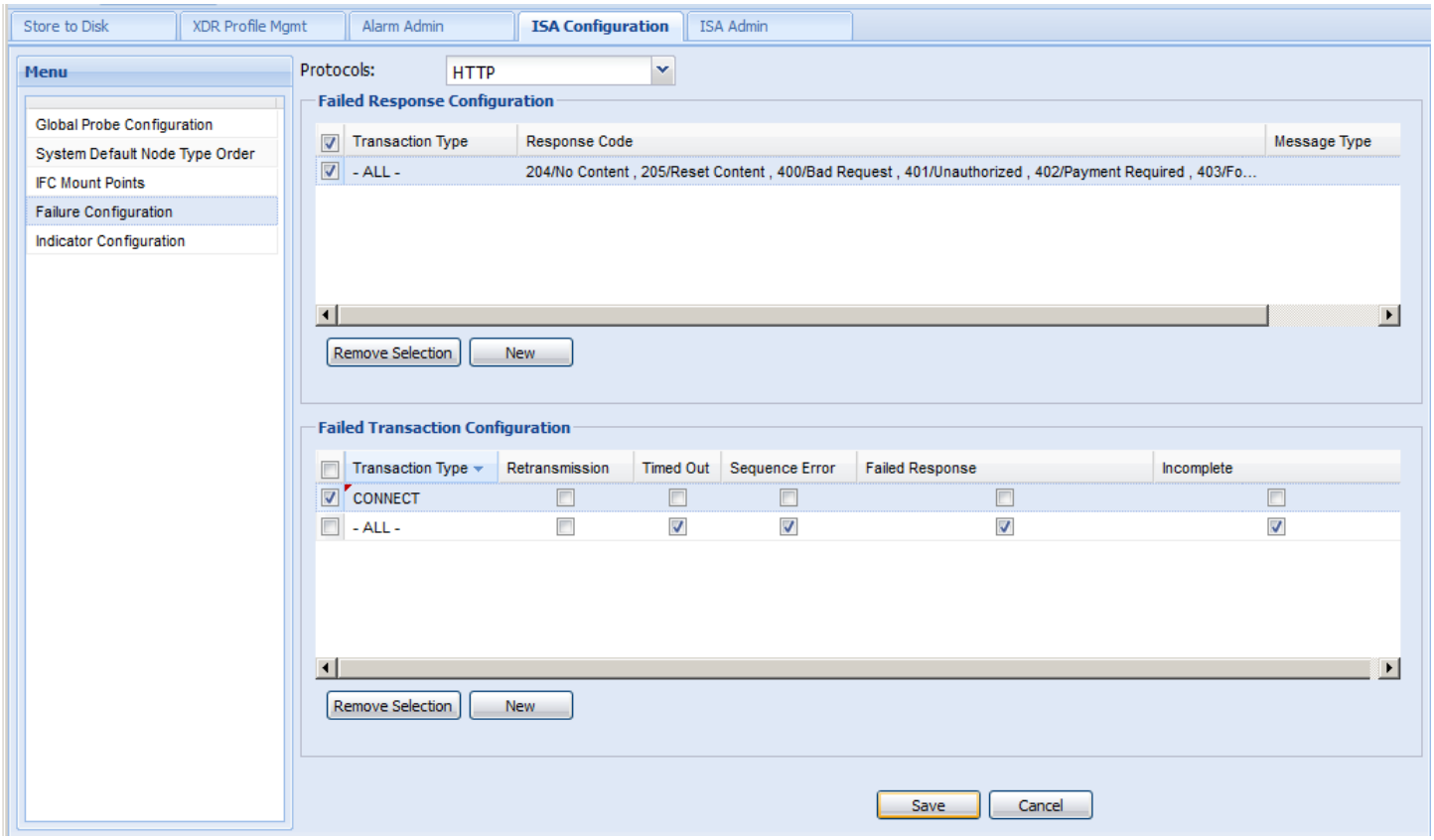
ISA Configuration Tab - System Default Node Order



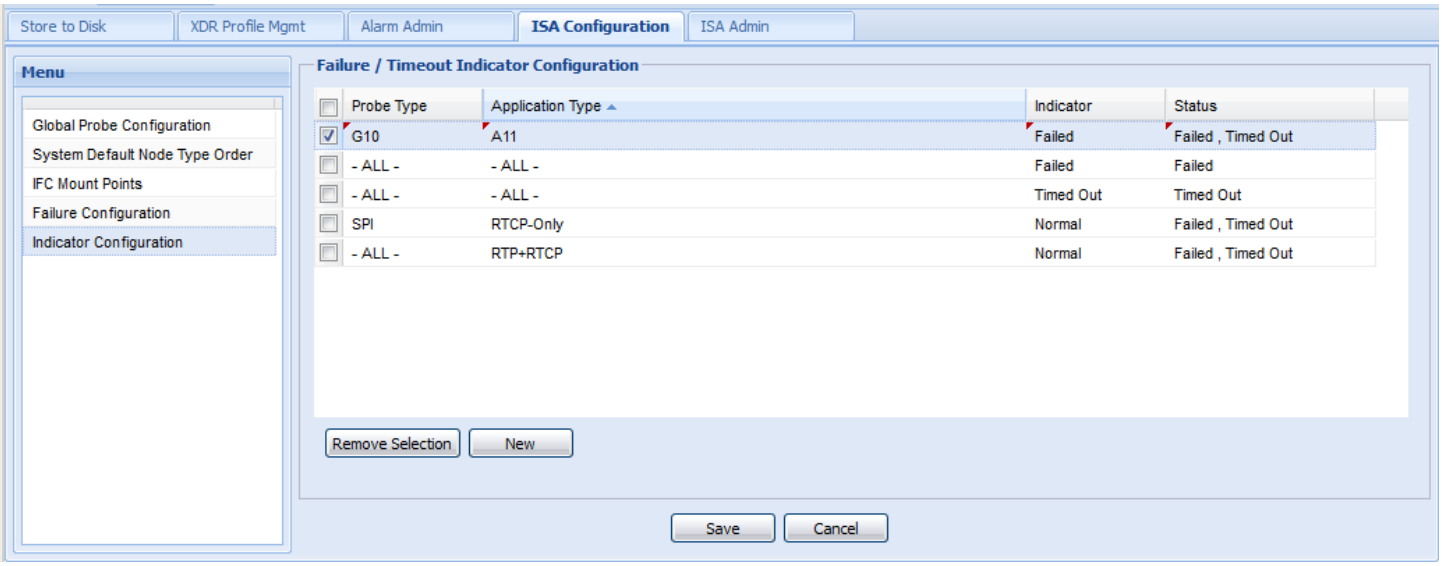
ISA Configuration Tab - IFC Mount Points Configuration



ISA Configuration Tab - Failed Response Configuration



ISA Configuration Tab - Failure/Timeout Indicator Configuration

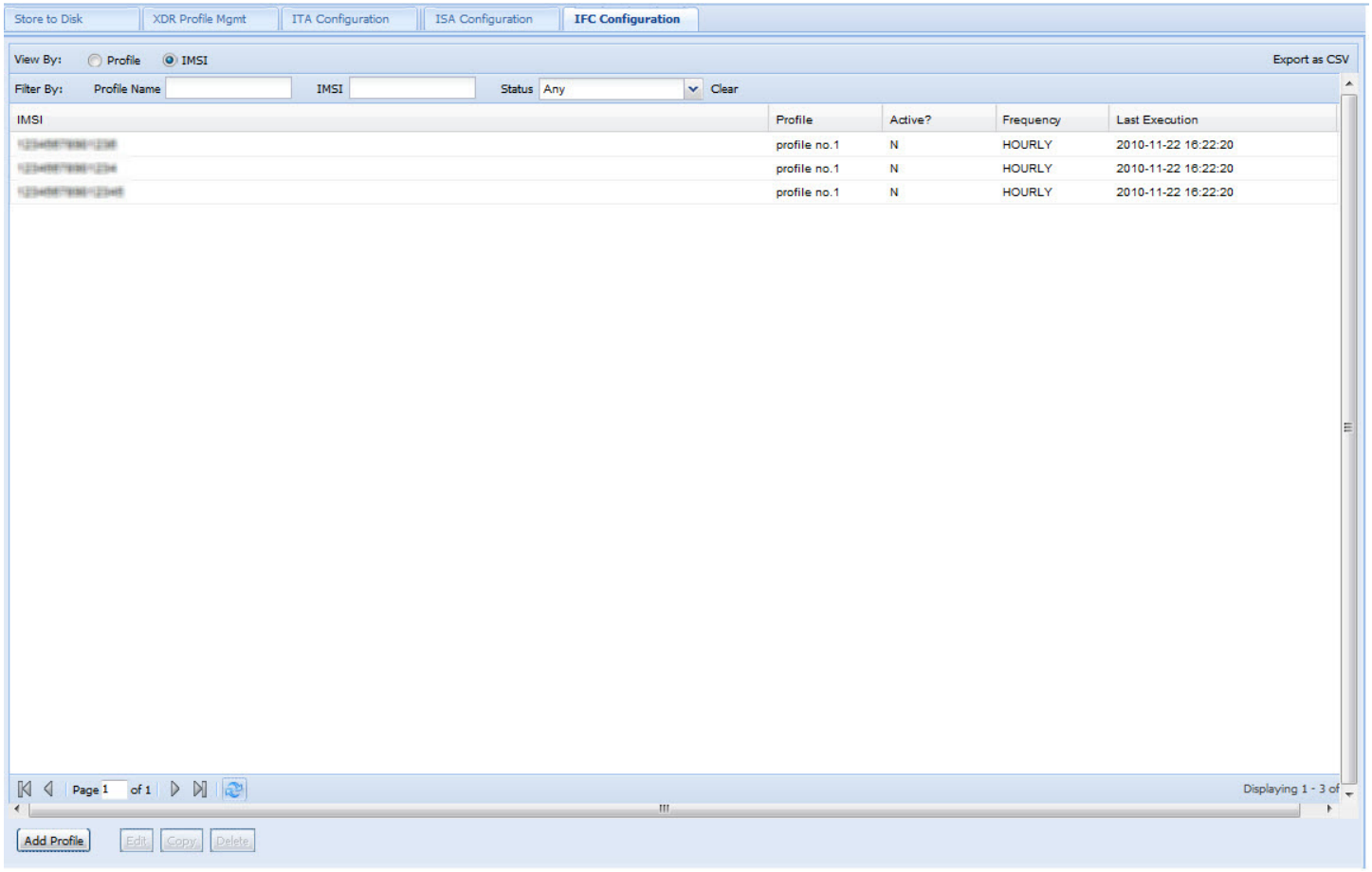


IFC Configuration Tab

The IFC Configuration tab enables you to set profiles to schedule session traces for customers of interest and save them to your local disk or a remote server repository. You can view the list of profiles by Profile name or by IMSI. When viewing by IMSI, every Profile to IMSI mapping will be represented by a row in the grid. For example, if an IMSI is present in multiple profiles, there will be multiple rows in the grid for that IMSI.

View By	View the scheduled list by profile name or by IMSI
Export as CSV	Export the list of profiles with accompanying detail information (Start and End Time, etc.)
Filter By	Filter the list of profiles by profile name, IMSI, or Status (Any, Active, Inactive)
Clear	Clear all filter elements
IMSI/Profile Name	Profile Name: View and sort IFC profiles by name. IMSI: View and sort IFC profiles by the IMSI.
Active?	Designates whether the profile is Active (Y) or Inactive (N)
Frequency	Designates how often the profile is scheduled to run
Last Execution	Lists the last time the profile was executed in YYYYMMDD HH:MM:SS
Add Profile Button	Opens the Profile Configuration window so you can add a new profile.
Edit Button	Edit the selected profile in the Profile Configuration window.
Copy Button	Copy the selected profile
Delete Button	Delete the selected profile; if you delete a profile while viewing by IMSI, you will delete the profile to which the IMSI belongs, not the IMSI from the profile. You can only remove an IMSI from a profile while in edit view.

IFC Configuration Tab



IFC Profile Configuration Window

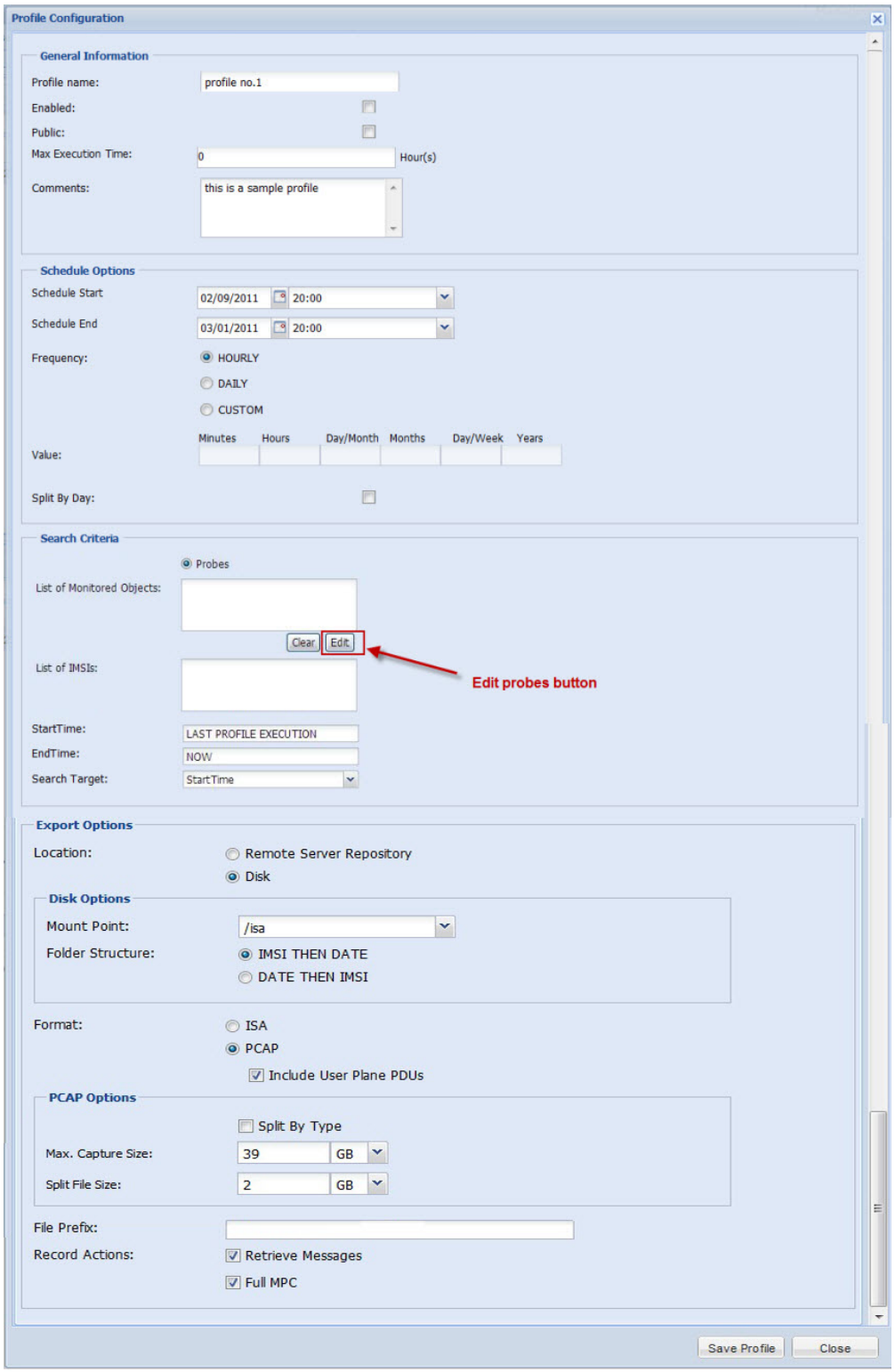
The IFC Profile Configuration window enables you to see the details for each profile. If a profile configuration is changed, the currently running job will not be affected; after the running jobs are finished, all future job executions will be based on the new profile configuration.

General Information	
Profile Name	Name given to the profile when it is created.
Enabled Check Box	Each profile can be enabled or disabled as needed. Only searches for enabled profiles will be scheduled and executed.
Public Check Box	Each profile can be designated as "public". If this checkbox is selected, the profile is stored in the public directory on the repository.
Max Execution Time	Define the number of hours a capture can run. The default value is 8 hours, and the maximum value is 24 hours. When the defined maximum execution time is reached, the running capture will stop executing without exporting any data and release all used resources.
Comments	Freeform field for comments on the profile.
Schedule Options	
Schedule Start	The scheduled start day and time for the search

Schedule End	The scheduled end day and time for the search
Weekday Only	Check box to designate that the traffic is only retrieved from Monday to Friday.
Frequency	How often the search is executed: Hourly, Daily, or Custom
Value	If Custom is selected for the Frequency, then enter a value for one of the following: • Minutes • Hours • Day/Month • Months • Day/Week • Years
Split By Day	Checkbox to split the retrieved traffic file by day to be saved.
Search Criteria	
Probes Radio Button	Conduct the search for Probes.
List of Monitored Objects	Displays the list of selected elements.
Clear/Edit buttons	Use the Edit button to display a dialog window with a list of probes to select. Use the Clear button to clear the field.
List of IMSIs	Each profile may have multiple IMSI filters, and one search job is created for each IMSI filter; one profile may generate multiple searches. The maximum number of enabled subscribers (IMSIs) is a licensing option.
Start Time	The Start Time the search profile uses
End Time	The End Time the search profile uses
Search Target	Determine what criteria to use for the search: Start Time, Active Time, or End Time
Export Options	
Location	The search results can be stored locally to disk or to the remote server repository.
Repository Options: Storage Duration	Storage time in days
Disk Options: Mount Point Folder Structure	• Specify where on the disk to store the search results • Determine how to store the search results: by IMSI then Date, or Date then IMSI
Format	• ISA - exports the IFC sessions to ISA session (.isa) files. • PCAP - exports the IFC sessions to PCAP files.
PCAP Options	
Include User Plane PDUs Check Box	Select this check box to specify that a PCAP export includes user plane PDUs.
Split by Type Check Box	Select this option to export a separate PCAP file for each of the following PDU types: • Wire (Raw) • Control Plane • IP Reassembled • L4 Assembled

Max Capture Size Field	Set the maximum number of bytes for all PCAP files exported. If the maximum capture size limit results in a truncated export, the user will be notified in the log that is returned with the PCAP file.
Split File Size	Set the maximum size for each PCAP file created from the split PCAP file.
File Prefix	Enter the prefix for the resulting file name.
Record Actions: Retrieve Messages, Full MPC	The record searches can be any combination of retrieve messages and a full MPC (multi-protocol correlation)

IFC Profile Configuration

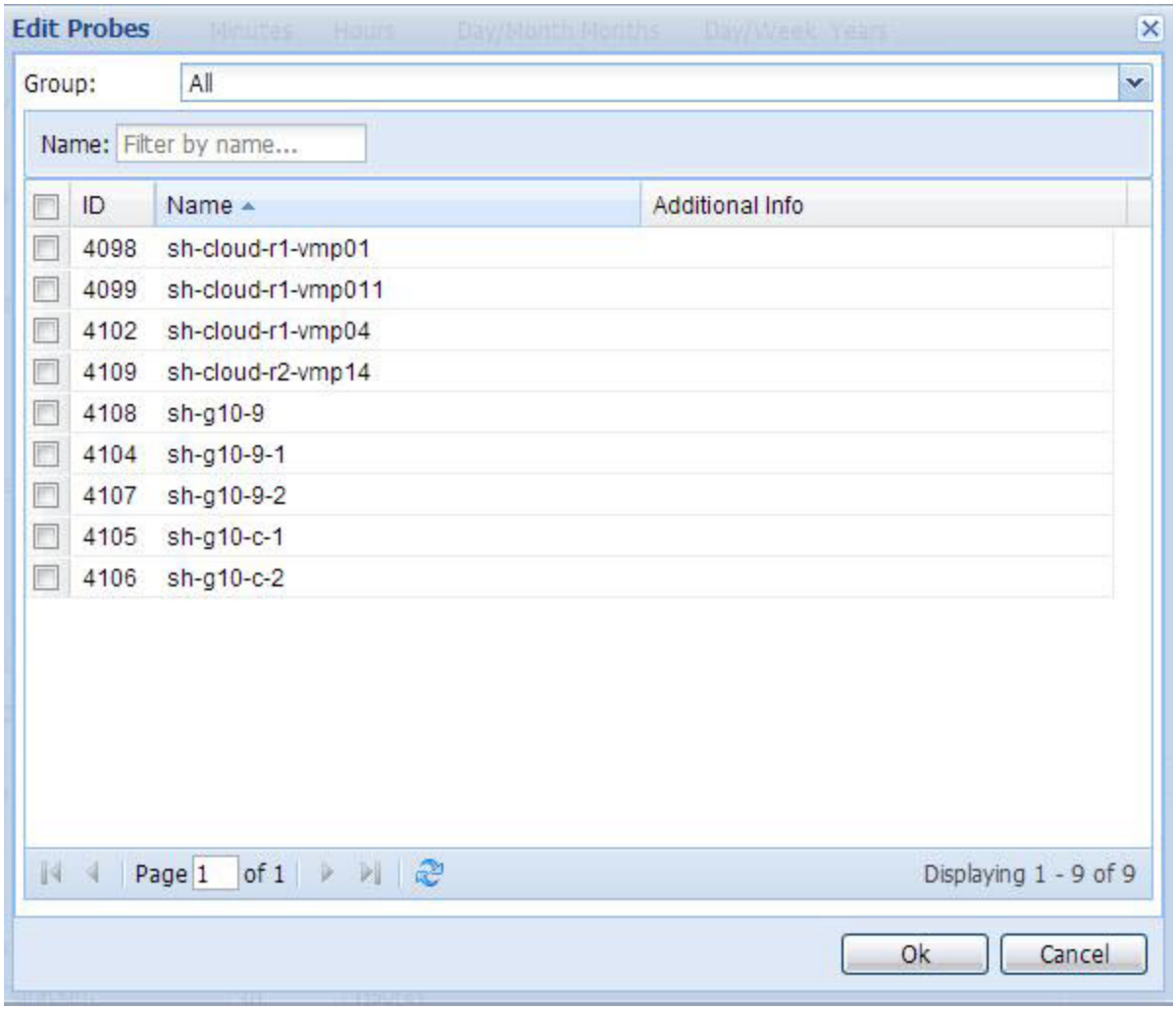


Edit Probes Dialog

The Edit Probes dialog box enables you to select probes from a list to add to the IFC Profile Configuration window. You can access this dialog from the IFC Profile Config window.

Group:	Select a probe group from the drop down list, or select All. You must select the probe(s) you want in the profile using the checkbox next to the probe name.
Name:	Filter the list of probes by name.
ID/Name columns	The probe ID and Names for each probe are listed. You can sort Ascending and Descending by Name.
Check box	Select each probe you want to add to the Profile using the check boxes next to the probe ID.
OK button	When you have added all the probes you want, click the OK button to return to the Profile Config window.
Cancel button	Use the Cancel button to exit out of the dialog without selecting any probes.

Edit Probes

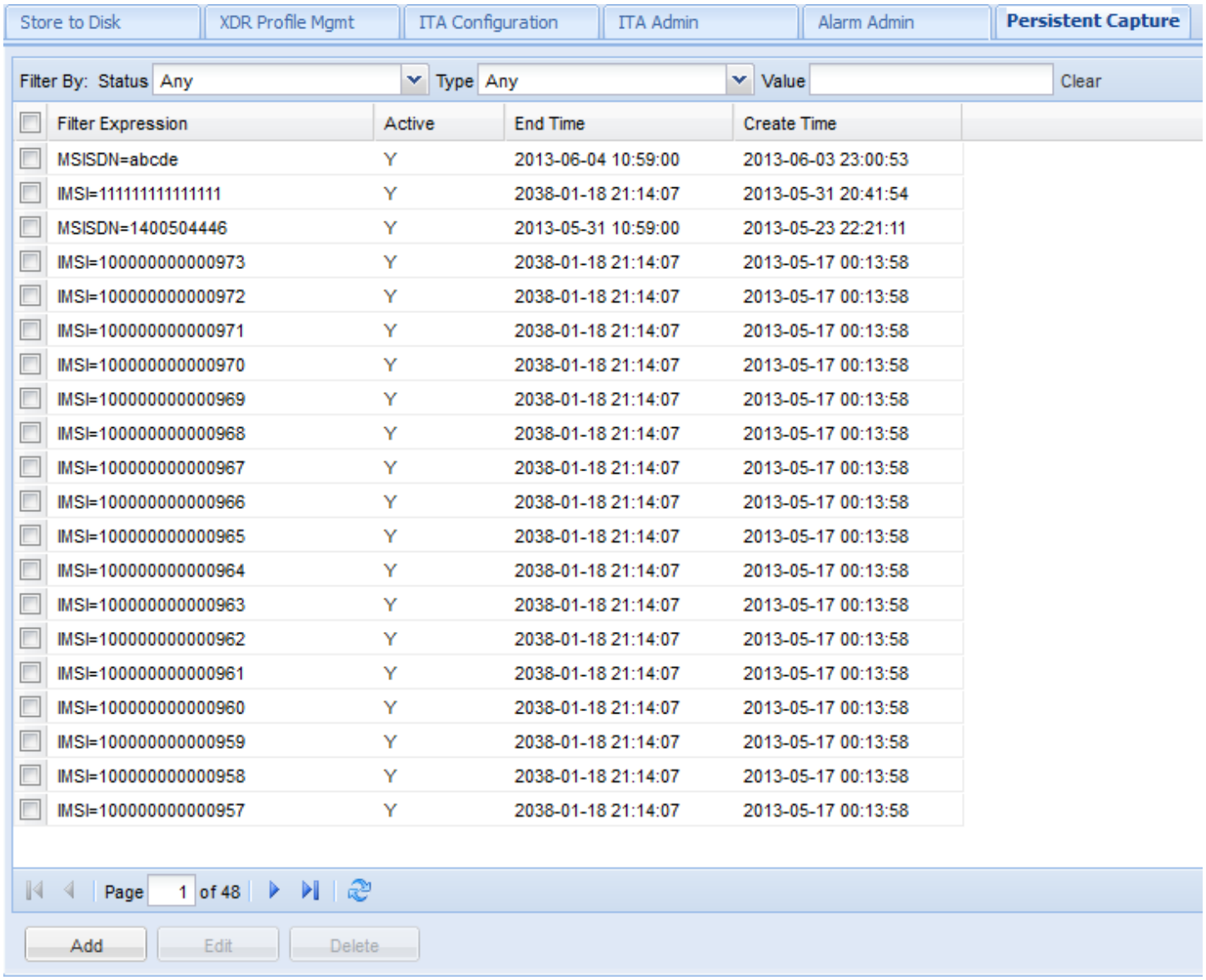


Persistent Capture Tab

The Persistent Capture tab enables you to set profiles to schedule long-running session traces of user plane data by IMSI or MSISDN.

Filter By:	Filter the data in the list by the following parameters: • Status - Active, Inactive, Any • Type - IMSI, MSISDN, Any • Value - Enter a specific IMSI or MSISDN number
Clear Button	Clear the current filter.
Filter Expression Check Box(es)	Click the top check box to select all of the persistent capture filters or select
Filter Expression Column	Contains the filter type, IMSI or MSISDN, and its specific value.
Active	Shows if the persistent capture is active or not: Y or N.
End Time	Scheduled end time of the persistent capture in HH:MM:SS format.
Create Time	Creation time of the persistent capture in HH:MM:SS format.
Page Controls	Go forward or backward one page, or go to the last or first page.
Add	Add a new persistent capture. When you click this button the Add Persistent Capture Filter dialog box appears.
Edit	Edit an existing capture. Select a capture and click Edit to open the Update Persistent Capture Filter dialog box.
Delete	Delete a selected persistent capture filter.

Persistent Capture Tab



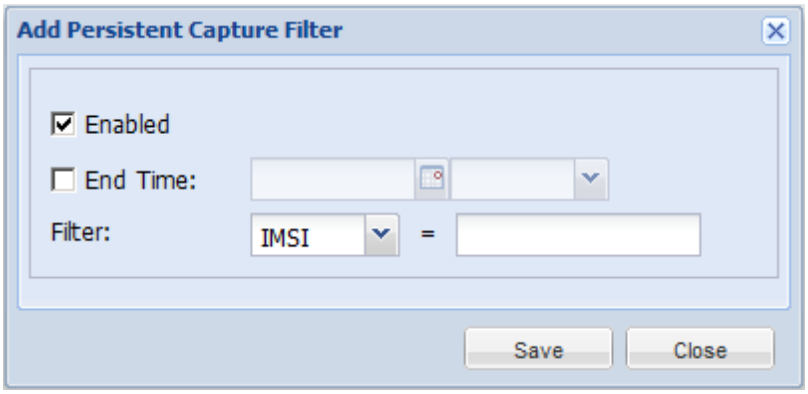
Add/Update Persistent Capture Dialog Box

When you click Add on the Persistent Capture tab, the Add Persistent Capture Filter dialog box appears. When you select an existing Persistent Capture profile and click Edit, the Update Persistent Capture Filter dialog box appears.

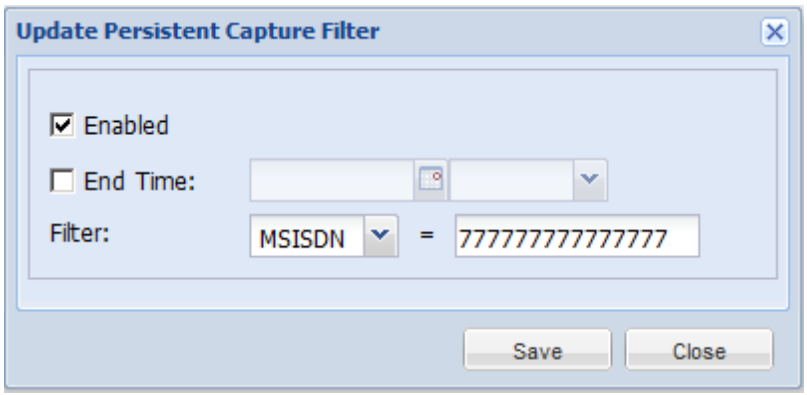
Enabled Check Box	Enable the persistent capture. When you click this check box, a "Y" appears in the Active column on the Persistent Capture tab. If you do not select this check box, a "No" appears in the Active column after you click Save and the dialog box closes.
End Time Check Box	Select to enable End Time options. This check box is deselected by default when you add a profile. If you are updating a profile, the check box can appear selected or deselected depending on whether or not an end time was specified.

End Time Options	Specify the following End Time options: • Select a date from the calendar icon or enter one in the field. • Select a time in 15-minute increments from the options menu or type any time you want in the field.
Filter	Select IMSI or MSISDN and then enter a value.
Save	Save your changes.
Close	Close the dialog box.

Add Persistent Capture Filter Dialog Box



Update Persistent Capture Filter Dialog Box



Licenses Tab

The Licenses tab enables you to view the license information for all configured Iris applications.

Licensed Application Column	Identifies the current Iris application licenses.
Version Column	Not used in this release.
Expired Date Column	The expiration date for the license.
Host ID Column	The Host ID of the computer associated with the license.

Licenses Tab

Iris Server License Information

Licensed Application	Version	Expired Date	Host ID
iris_application_ipi	1.0	20-jul-2012	[illegible]
iris_application_ondemand	1.0	20-jul-2012	[illegible]
iris_application_ipa	1.0	20-jul-2012	[illegible]
iris_application_cac	1.0	20-jul-2012	[illegible]
iris_application_ita	1.0	20-jul-2012	[illegible]
iris_application_ace	1.0	20-jul-2012	[illegible]
iris_application_isa	1.0	20-jul-2012	[illegible]

Probes User Interface

Admin contains the following Probes GUI elements.

- Probes Tab
- Probe Details Tab
- Timing Control Tab
- Monitoring Details Tab
- Media Configuration Tab
- gSoft Configuration Tab
- ISA Configuration Tab
- Storage Maintenance Tab
- TD140 Ports Tab
- TD140 Details Tab
- TD140 Managed Probe Tab

Probes Tab

Once G10 probes and other devices are installed and configured to communicate with the Iris server, system administrators can manage them using the Probes tab. Devices managed from the Probes tab include:

- G10 probe
- TD140 Traffic Distributor
- GeoSoft RAN probe

SpIprobes are configured and maintained using the GeoProbe UI. Refer to the GeoProbe product documentation for more information about SpIprobes.

Probe List Pane

View all provisioned devices that have communicated with the Iris server: G10, TD140, GeoSoft RAN.

Name Filter	Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive. • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Type Filter	Select a probe type to filter the probe list. The available tabs vary depending on probe type.
Group Filter	Select a probe group name to filter the probe list. The drop-down menu lists all entity groups defined on the Groups Tab. Group names display in the format [Group Entity] - [Group Name].
Connection Status	Select a connection status as a filter: **All** • View all provisioned probes; both connected and disconnected. **Not connected - Element name appears in gray text** • Element is not available for configuration or updates. • G10 and gSoft: Indicates **either** the probe SwManager connection or the ConfigServer connection is down. • TD140: Indicates the ConfigServer is down. **Connected - Element name appears in black text** • G10 and gSoft: Indicates **both** the ConfigServer and SwManager are up and running, and connected to the Iris server. • TD140: Indicates the ConfigServer is up and running and connected to the Iris server.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.
Statistical Counter	The counter shows the total number of provisioned devices (G10s, TD140s, gSoft probes) and the number of connected devices. G10s bound to TD140s are also included in the count.

Probes Tabs (G10 and GeoSoft)

The following tabs appear when you select either a G10 probe or a GeoSoft RAN probe in the Probe List pane. The available tabs vary depending on which probe type you select.

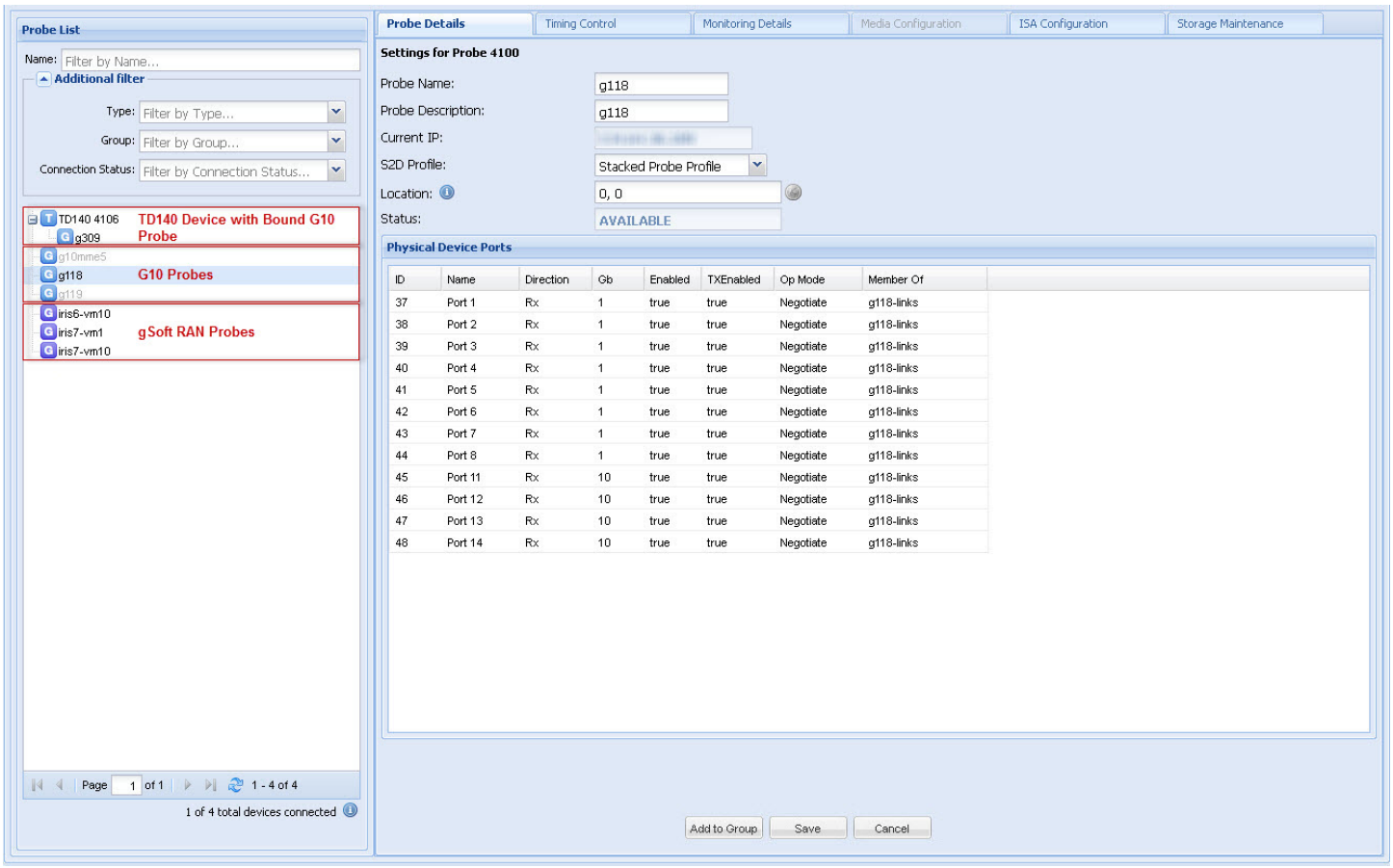
Probe Details Tab	Configure probe settings including name, description, and physical device ports.
Timing Control Tab	Customize timing references per G10 probe. See G10 Probe Timing for details.
Monitoring Details Tab	***This tab only applies to G10 probes.*** Configure per-probe configuration settings and view currently monitored nodes.
gSoft Configuration	***This tab only applies to GeoSoft RAN probes.*** Configure probes setting for the GeoSoft RAN probe.
Media Configuration Tab	Configure the type and quantity of RTP media you want to capture for the Comprehensive RTP Media Capture feature. This is a licensable feature and must be enabled by a Tektronix Engineer.
Storage Maintenance	The Storage Maintenance tab is reserved for Tektronix technical support. See Storage Array Configuration for details. ***Do not change the Storage Maintenance settings, as this can result in loss of data or system configuration.***

TD140 Tabs

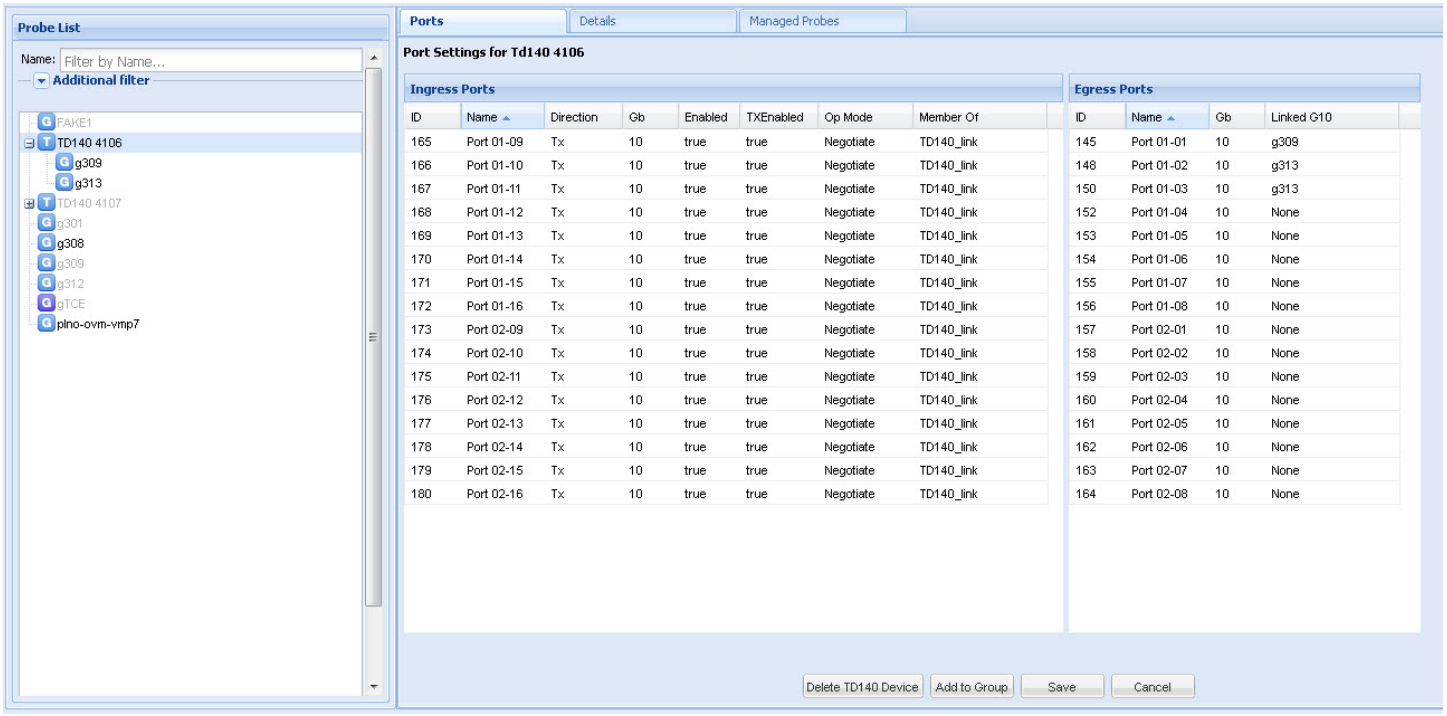
The following tabs appear when you select a TD140 device in the Probe List Pane.

TD140 Ports Tab	Define ingress and egress port settings for the TD140.
TD140 Details Tab	Configure TD140 settings including timing and load balancing.
Managed Probes Tab	Configure settings for G10s bound to a TD140 device including traffic type, session allocations, and maximum packets per second received.

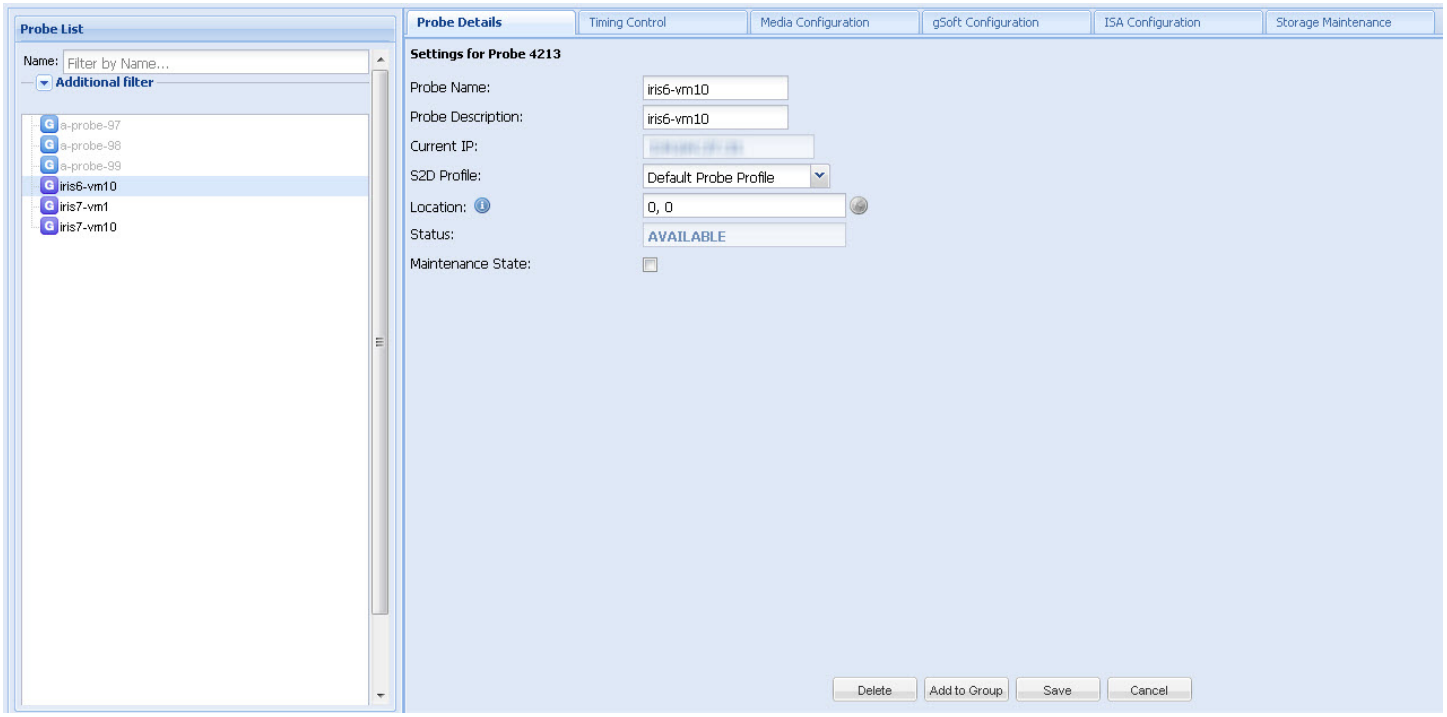
Probes Window (G10 Selected)



Probes Window (TD140 Selected)



Probes Window (GeoSoft RAN Selected)



Probe Details Tab

The Probe Details Tab enables you to configure probe settings and physical device ports. You select the probe you want to view in the Probe List pane.

Probe Details Area

Settings for Probe 4XXX	Unique number that identifies every provisioned probe. During initial probe installation, the Iris server assigns the first probe an ID of 4097; subsequent probes are numbered sequentially 4098, 4099, etc. This ID is seen in Iris applications as well as in alarms.
Probe Name Field	Rename a probe as needed. When the probe is first configured, the Probe ID appears as the probe name. This name is seen in Iris applications as well as in alarms.
Probe Description Field	Assign a label to a probe for easier management.
Current IP Field	View the IP address that was configured on the probe at installation. You cannot modify this field.
S2D Profile Field	Set configuration for storing probe data to disk. See Store to Disk Tab and Managing Iris Data Storage for details.
Location	Enter a city name to search by city or the Latitude and Longitude coordinate for the location you want the element to appear on the map. Various Internet sites provide longitude and latitude coordinates when you enter address information. • Valid latitude coordinates are between -90 and 90 • Valid longitude coordinates are between -179.99 and 179.99 • Lat/Lon values separated by a comma or semi-colon can be copied from a source (such as the Internet) and pasted into either field; Iris automatically separates the values into separate fields • If no coordinates are defined, Iris will assign the default longitude and latitude values set in the Locations Tab. • You can also change a probe's Lat/Lon values directly from the Iris Maps Overview window. Refer to the Iris Online Help for details. The Location icon indicates how the coordinates were set: • Gray - coordinates set by system based on mapping rules configured in the Locations Tab. The settings will automatically be updated with any changes to the Location rules or you can manually update the coordinates in this pane or directly on the map. • Green - coordinates were manually set; the settings will not be overwritten by updates to the Location rules.

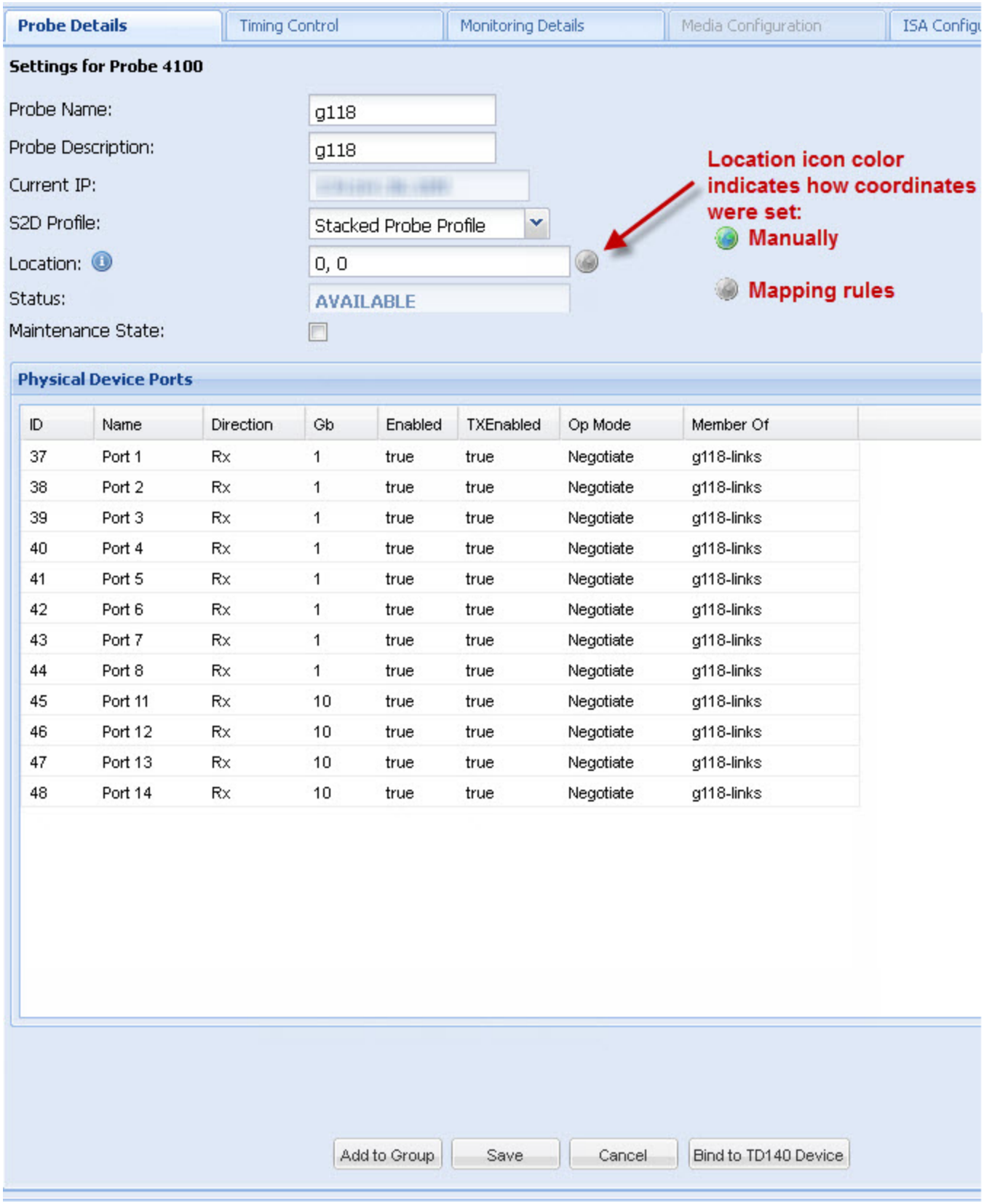
Status Field
 	
Maintenance State Check Box
	• Click the Maintenance State check box to enable/disable a probe's maintenance status. This check box is only visible:
	  • To users with the Admin privilege
	  • If the current probe is not bound with a TD140. Maintenance status for probes bound to a TD140 is controlled by the TD140 maintenance status.
	• Status field Indicates whether the probe is AVAILABLE or in a MAINTENANCE state. When a probe is in a maintenance state:
	  • System alarms for the probe are not generated
	  • Nodes and logical links being monitored by a probe in a maintenance state will also be placed in a maintenance state; their associated LDV policy-based alarms will not be generated. Refer to the Iris online help for more information about LDV policy-based alarms.

Physical Device Ports Area [G10 Probes Only]

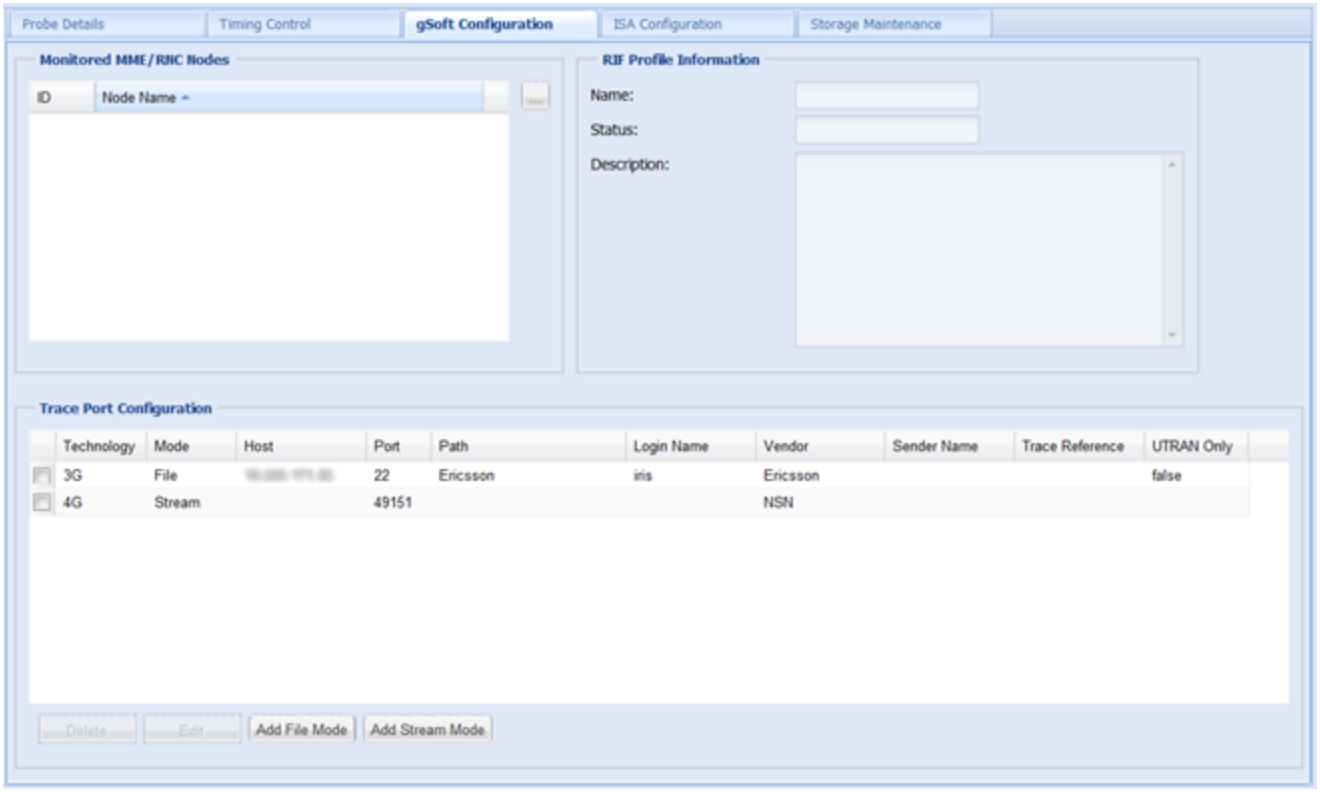
ID Column	An internal identifier used by the Iris server. The ID is assigned in the order of probe registration with the server. The first probe registered uses port IDs 1-12, and subsequent probes are assigned port IDs 13-24, 25-36, etc.
Name Column	The default name is Port n, where n indicates the physical port number. This column always shows the default port names even though not all will be configured. Tektronix recommends not editing the name of the port. If you edit the name of the port, ensure you can identify the physical port and its corresponding physical location it represents on the probe itself.
Direction Column	Set the proper direction for each G10 probe port: RX, TX, or Span (bidirectional). These settings depend on whether the monitored network physically connects to the G10 via span/mirror ports or optical splitters. • **Optical Tap/Splitter Ports:**these connections can only monitor in one direction, so **RX** or **TX** are valid options. • **Span/Mirror Ports:**these connections can monitor in any direction, so **RX**, **TX**, or **Span** are valid options. Refer to Physical Device Port Configuration Examples for more information.
Gb Column	The capacity of the link rate, which can be 1 Gbps or 10 Gbps, depending on the probes you are using. Iris supports various combinations of 1G and 10G ports on the same probe; refer to Monitored Link Support for details.The number of displayed ports varies depending on the hardware configuration of the probe: • **IIC100** - Ports 1-8 are reserved for the IIC100 1G ports; Ports 11-14 are reserved for the TRM100 RTM 10G ports. Refer to IIC100 Physical Device Port Configuration Examples for more information. • **IIC200** - Only ports 1-8 are visible. Ports 1-4 only support 1G Ethernet connections; ports 5-8 are dual-purpose sockets which can be used for either 1G or 10G Ethernet connections. Refer to IIC200 Physical Device Port Configuration Examples for more information.
Enabled Column	Enable or disable the link for monitoring. Initially this column has a "true" value (port Enabled). When you click on it, the text is replaced by a checkmark. Clear the checkmark to set the port to "false" (port Disabled).
TX Enabled	Enable or disable light transmission from the G10 TX port. Set this field based on whether the ports are physically configured to support span ports or tap ports. Refer to Physical Device Port Configuration Examples for more information. • **Span Ports**: TXEnabled=**TRUE**. Span ports require the G10 transmit light from the TX port to keep the port active. • **Tap Ports**: TXEnabled=**FALSE**. Tap ports do not use the TX port and you can disable it.

Op Mode	Select one of the following options for 1G ports. Op Mode is disabled for 10G ports: • **Negotiate** - enables this port to auto-negotiate speed and duplex abilities with client-side ports. • **Full-duplex** - enables communication in both directions, simultaneously. • **Half-duplex** - enables communication in both directions, but only one direction at a time. Set this field based on whether the 1G port is physically configured to support span ports or tap ports. Refer to Physical Device Port Configuration Examples for more information. • **1G Span Ports**: Op Mode=Negotiate; select Full Duplex or Half Duplex only if the monitored equipment is not configured to auto-negotiate. • **1G Tap Ports**: Op Mode=Full Duplex is recommended for most configurations; Half Duplex may be required in certain configurations.
Member Of Column	View the physical link that maps to this port, if any. This field is auto-populated when you configure physical links on the Topology Tab; you cannot modify it. See Configuring Physical Links for details.
Add to Group	Open the Add to Group dialog box and select a group name from a list of existing groups created on the Groups Tab. Groups in which the probe is already a member are not listed for selection. Group names display in the format [Group Entity] - [Group Name].
Save Button	Save all current probe and device port settings.
Cancel Button	Close the Probe Settings pane without saving changes.
Bind to TD140 Device	Bind the selected G10 probe to a TD140 device. This button is only visible if at least one TD140 device has connected to the Iris server. A confirmation dialog box appears for you to confirm you want to bind the selected TD140 device. Once confirmed, a TD140 Selector dialog box appears for you to select the parent TD140 and the traffic type for this probe. The G10 is moved under the TD140 device in the tree view.
Unbind from TD140 Device	***If you need to unbind a G10 from a TD140, first ensure the G10 is not currently being upgraded during execution of a software campaign.*** Unbind the selected G10 probe from a TD140 device. This button is only visible if you select a G10 that is bound to a TD140 device. The G10 is removed from under the TD140 device in the tree view.

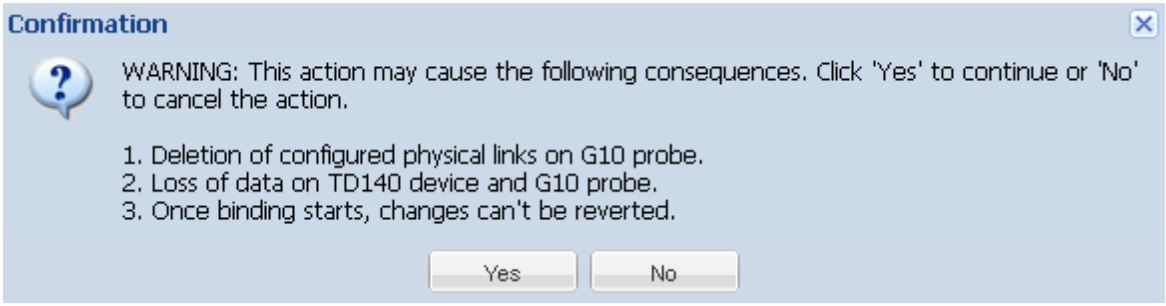
Probe Details Tab [G10 Probe]



Probe Details Tab [gSoft RAN Probe]



Bind G10 to TD140 Device Confirmation Dialog Box



Select TD140 Device Dialog Box

Timing Control Tab

The Timing Control Tab enables you to customize timing references per G10 probe. See G10 Probe Timing for details.

- Customize the list of NTP servers that a probe uses for timing reference
- Configure IRIG timing to and between G10 probes. A G10 probe can operate as an IRIG master or an IRIG slave. See G10 Probe Timing for details and hardware requirements.

Timing Control Tab

NTP Servers Field	• **default** - indicates the probe is using the default system-level NTP server list for timing reference. System-level NTP servers are configured on the Servers tab. • **custom** - indicates the probe is using a customized NTP server list for timing reference. You can customize the default list by deselecting one or more NTP servers for this probe or by defining additional NTP server IP addresses using the Select NTP Servers Dialog Box. • **changed** - indicates NTP server settings have been customized in the Select NTP Servers Dialog box, but are not yet saved. • **resetting** - indicates a reset to NTP defaults action is pending but not yet saved. • To customize the NTP servers list for this probe, click the NTP Servers field or the ellipsis (...) button to open the Select NTP Servers Dialog Box.
IRIG Status Field	***Probes require minimum software version 13.1 to support IRIG timing. See G10 Probe Timing for details and hardware requirements.*** • **Disable** - IRIG timing disabled for this probe. NTP timing will be used. • **Master** - this probe is designated as the IRIG master and will provide IRIG timing to all probes configured as slaves to this probe. The master probe receives its timing source from the defined NTP servers. • **Slave** - this probe is designated as an IRIG slave and will receive IRIG timing from the probe defined in the IRIG Master field. Slaves use NTP timing source for time of day reference.
IRIG Master Field	***Probes require minimum software version 13.1 to support IRIG timing. See G10 Probe Timing for details and hardware requirements.*** • Field displays when the IRIG status field is set to Slave. • Select from a list of probes designated as IRIG Master, or type the name of the IRIG Master probe. • If using a device such as a GPS device as a timing source, type the name of a master time source. Spaces are not allowed.

Select NTP Servers Dialog Box

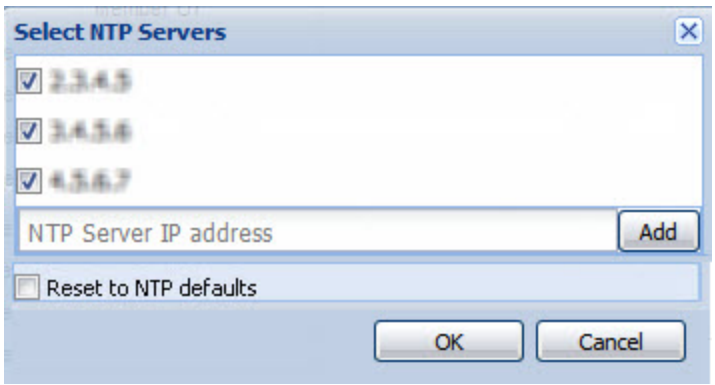
- Use this dialog box to view or customize the NTP server list defined on the System tab.
- If no changes are made to a probe's NTP server list, then it inherits any changes made to the system-level NTP server list on the System tab.

IP Address checkboxes
 	
NTP Server IP Address Field
 	
Add button
	• Lists all NTP servers defined on the System tab. By default, all defined NTP servers are selected for a probe.
	• Deselect IP addresses for NTP servers you do not want the G10 to use for timing reference.
	• Enter additional IP addresses in the text field and click the Add button to add NTP servers for this probe.
	  • New entries added to the list appear with a checkmark.
	  • If you add an IP address and later deselect it (clear the checkmark), the value is not stored in the dialog box and you must re-enter the IP address.

Reset to NTP defaults checkbox	Enables you to remove any customizations and reset the probe's NTP server list to the default server list defined on the System tab.

Timing Control Tab

Select NTP Servers Dialog Box



Monitoring Details Tab

The Monitoring Details Tab enables you to view currently monitored nodes and set various per-probe settings. You select the probe you want to view in the Probe List.

Auto Node Topology Commit Enabled Check Box	Controls whether new or updated nodes are automatically added to the Iris system for the selected probe. Default is Enabled. **Enabled** • Newly discovered nodes are committed by the Iris Server to the master topology and the Topology Tab is updated. • Per-probe nodes are associated with the probe that discovered them. You can view probe-to-node associations for per-probe nodes on the Provisioning tab on the Node Details Pane. • Iris server continues to update probe associations for **existing** per-probe nodes. • Auto-detected element updates are logged in the Audit Log. **Disabled** • Newly discovered nodes are NOT added in the system; the server will not add any new nodes (even per-probe nodes) discovered by the probes. • Iris server continues to update probe associations for **existing** per-probe nodes. Tektronix recommends keeping this option enabled to ensure new nodes that are added to your network are auto-detected and included in the Topology Tab so they are available for use in Iris applications. To enable/disable this setting for all probes, see the Auto Detection Tab in Topology.
Auto Link Topology Commit Enabled Check Box	Controls whether new or updated links are automatically added to the Iris system for the selected probe. Default is Enabled. **Enabled** • Newly discovered links are committed by the Iris Server to the master topology and the Topology Tab is updated. • Auto-detected link updates are logged in the Audit Log. **Disabled** • Newly discovered links are NOT added in the system; the server will not add any new links discovered by the probes. Tektronix recommends keeping this option enabled to ensure new links that are added to your network are auto-detected and included in the Topology tab so they are available for use in Iris applications. To enable/disable this setting for all probes, see the Auto Detection Tab in Topology.
Session Tracking Enabled	This setting only applies to G10 standalone probes. Default is Enabled. **Enabled** • Probe sends data to the traffic processor to create session records in ISA and DRs. • Probe supports ISA and ITA in normal operation (default configuration). **Disabled** • Probe does NOT send data to the traffic processor to create session records in ISA and xDRs • Probe **only** supports PA, and ITA transport KPIs for Control Plane traffic.

Session Tracking Display Enabled	This setting can only be enabled if Session Tracking Enabled option is ON. This setting only applies to G10 standalone probes. Default is Enabled. **Enabled** • Probes are available for selection in the ISA Filter, Forensic capture profile and ISA API filter window. **Disabled** • Probes are NOT available for selection in the ISA Filter, Forensic capture profile and ISA API filter window. • Probe's traffic processor process will end the existing session and block further incoming requests for the disabled probe.
User/Control Plane Split Support	Enable or disable GTP split monitoring for the current probe. When this feature is enabled, you must configure separate GTP-C and GTP-U XDR profiles and assign them to this probe.
IPSec Support on Gm Interface	Enable IPsec decryption on the Gm interface. IPsec encryption provides security protection for network traffic. The G10 supports the deciphering of IPsec traffic on a Gm interface to allow for monitoring of the deciphered traffic. For the Gm interface, the deciphering keys are on the Mw interface and must be monitored by the G10. The IPsec deciphered traffic is processed by the G10 and Irisview applications in the same manner as clear text traffic. This feature requires an IPSec license and a G10 probe with an IIC100/IIC200 having 8G memory or greater.

HTTP Pipelining Support	Enable HTTP pipelining support for this probe. **This setting can only be enabled if the probe is configured with an IIC200.**
	
	HTTP pipelining is a method in which multiple HTTP requests are sent on a single TCP connection without waiting for the corresponding responses. Since several HTTP requests fit in the same TCP packet, HTTP pipelining allows fewer TCP packets to be sent over the network, reducing network load.
	
	Enabled
	• Probe supports monitoring of HTTP pipelining traffic in session records and DRs.
	• Pipelining HTTP transactions statistics are reported in ITA. For details about configuring nodes for tunneling protocols, see the IP Range description in the Node Details Pane.
	• ISA displays pipelining traffic as follows:
	  • Ladder Diagram: as "HTTP(P)"
	  • Flow details: New line item, "HTTP Pipelining: [True or False]"
	  • PDU details: Shows decoded HTTP pipelining PDUs and a new HTTP Pipelining column appears, indicating True for pipelining flows
	• HTTP pipelining PDUs are decoded by PA.
	• Pipelining HTTP/TCP segments are truncated at the end of the last header. See also G10 Truncation.
	
	Disabled
	• Probe still captures HTTP pipelining traffic in session records and DRs, but the IIC200 will stop reporting transactions for a flow once pipelining is detected.
	• ISA/PA effects:
	  • ISA still indicates whether HTTP traffic is pipelining or not.
	  • HTTP pipelining PDUs are still decoded in ISA/PA.
	• ITA effects:
	  • Pipelining HTTP transactions statistics not reported.
	  • IIC200 marks the HTTP pipelining traffic as having holes in the TCP sequence to indicate to ITA that it should not count the HTTP pipelined requests as transactions.

TCAP Tracking Based on TID Only	Enable TCAP transaction tracking based on Transaction ID (TID) only. The default behavior is transaction tracking based on NodeID + TID.

Content Removal Enabled	This option is only visible when the Content Removal license is installed. **Enabled** • ***This feature requires a DC archive for data storage. See Content Removal Enabled Option - Affect on G10 Storage for details.*** • G10 removes subscriber SMS payload within SIP messages and MSRP content and replaces it with 0xff before storing it to disk. • ISA users with the User Content Capture privilege can override this option and start text captures within ISA to capture complete messages. Users with the User Content Visible privilege can view the complete messages; users without the User Content Visible privilege can only view the masked message. **Disabled** • G10 retains subscriber SMS payload within SIP messages and MSRP content. • ISA and PA users with the User Content Visible privilege can view the complete messages; users without the User Content Visible privilege can only view the masked message. This option also controls how SIP SMS and MSRP packets are stored on the G10 probe. See Content Removal Enabled Option - Affect on G10 Storage for details.
SMS Full Content Enabled	This option is only visible when the Content Removal license is installed. This option can only be enabled when the Content Removal Enabled option is also enabled (checked). **Enabled** • SIP messages are always stored in short-term archive. • All SIP messages are duplicated (one copy with SMS content and one copy without SMS content) • PA and ISA users with the SMS Full Content privilege can view the complete messages; users without the SMS Full Content privilege can only view the masked messages. See also SMS Full Content Enabled - System Impact for details. **Disabled** • G10, ISA, and PA behavior follows Content Removal Enabled settings.
Diameter Routing Agent Probe	Enable DRA monitoring for this probe. When you enable this feature, DRA-specific processing is enabled and S6a LTE mapper functionality is disabled (mapper updates are not needed). A selection field appears for you to select a DRA node. You must configure DRA nodes in the Topology Managed Objects Tab for them to be available for selection. DRA nodes in the list appear in gray text if they are already selected by another probe. **Select a DRA node** if you want the G10 to: • Monitor **both** ingress and egress sides of the DRA node. • Correlate ingress/egress transactions in a single session record and a single DR. **DO NOT select a DRA node** if you: • Do not need to correlate the ingress and egress DRA traffic. The G10 will monitor exclusively the ingress side or exclusively the egress side of the DRA. (Probe placement and interfaces being monitored define which side of the DRA is monitored.) • Are monitoring DRA ingress and egress traffic on separate G10 probes. ***NOTE:*** *It is assumed that the Diameter Client (MME, PGW) is monitored by a separate probe and is unchanged by the DRA probe's deployment. The Diameter Client probe generates DRs for the Diameter Client to DRA leg.*

Save Button	Save settings. Probes send topology updates to the Iris server every 5 minutes. If enabling auto topology detection for this probe after being disabled, elements that were previously detected are committed by the Iris server to the master topology and the Topology Tab is updated.
Cancel Button	Close the Monitoring Details tab without saving changes.

Content Removal Enabled Option - Affect on G10 Storage

Probe Type	Content Removal Enabled Option OFF	Content Removal Enabled Option ON

Standalone G10	• Stored as-is by Iris Interface Card (IIC) or Iris Applications Blade (IAP), depending on configured S2D profile.	• SMS content is replaced with 0xFF.
		• Stored by IAP to the DC archive. If no DC archive is configured, do one of the following:
		  • Reconfigure a ST or LT storage as a DC archive to avoid data loss
		  • Add disks, and configure as a DC archive to avoid data loss.

Media Probe **without** Comprehensive Media Capture	• Stored as-is by IIC or IAP, depending on configured S2D profile.	• SMS content is replaced with 0xFF.
Media Probe **with** Comprehensive Media Capture	• Stored as-is by IIC or IAP, depending on configured S2D profile.	• SMS content is replaced with 0xFF.
Control Plane Probe	• Stored as-is by IIC or IAP, depending on configured S2D profile.	• SMS content is replaced with 0xFF.

DPI Area

This check box is only visible with a DPC license and when the probe has the proper hardware (IAP200 and the 10G Interface cards). A check box allows you to enable/disable the Deep Packet Classification feature.

You configure traffic classification on the Protocol Details pane and the Application Details pane on the Topology Tab. Refer to the ***Traffic Classification Configuration*** tutorial in the Admin online help for workflow details.

Monitored Nodes Area

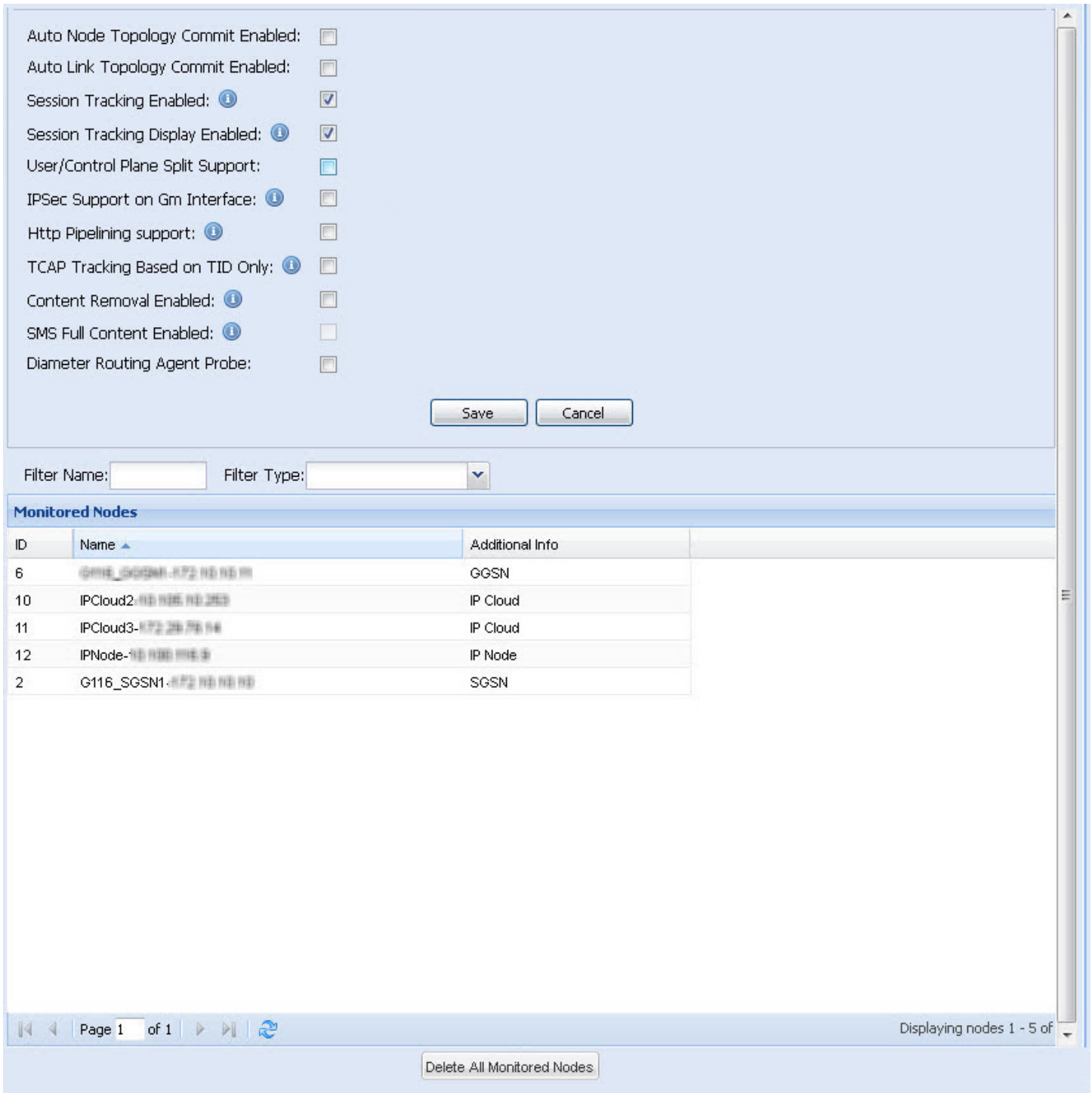
Filter Name Field	Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Filter Type Drop-Down Menu	Select a node type to use as a filter for the Monitored Nodes table.
ID Column	An internal identifier used by the Iris server. The ID is assigned in the order of node registration with the server, whether auto-detected or manually configured.

Name Column	Lists the names of the nodes being monitored by the selected probe. Node names are modified in the Node Details pane or using the Node Import Feature (see Using CSV File Import/Export for details).
Additional Info Column	Displays node type. Node names are modified in the Node Details pane or using the Node Import Feature.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.
Delete All Monitored Nodes	Delete existing monitored node associations. The probe resets monitored node associations after it receives traffic related to the nodes.

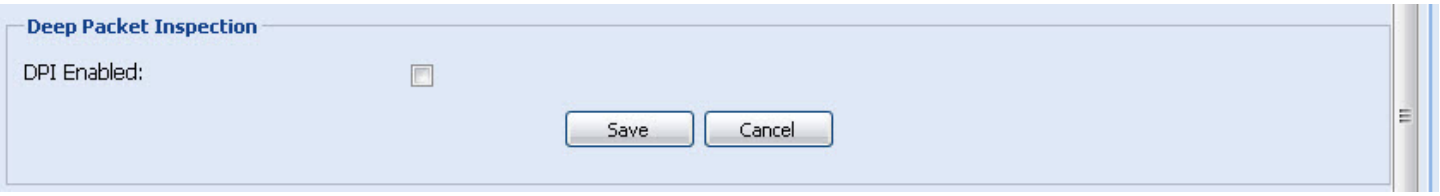
Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the check mark from columns you want to hide. At least one column must remain visible.

Monitoring Details Tab



Monitoring Details Tab - DPI Area



Diameter Routing Agent Probe - Select a DRA Node Field

SMS Full Content Enabled - System Impact

This feature enables full SMS payload content, within SIP messages, to be stored in the G10 probe for a short-term duration and is only visible with the PA and ISA application. This allows PA and ISA users to see all SMS content for troubleshooting purposes. System impact varies depending on configured per-probe parameters and user privileges.

PA Impact

"Content Removal Enabled" Parameter	"SMS Full Content Enabled" Parameter	"SMS Full Content" User privilege Enabled	"SMS Full Content" User privilege Disabled
Enable	Enable	Masked and original traffic (from long-term and short-term archives)	Masked traffic (from long-term or DC archive)
Enable	Disable	Masked traffic (from long-term or DC archive)	Masked traffic (from long-term or DC archive)
Disable	Enable/Disable	Original traffic from the archive configured in S2D profile	Original traffic from the archive configured in S2D profile

ISA Impact

"Content Removal Enabled" Parameter	"SMS Full Content Enabled" Parameter	"SMS Full Content" User privilege Enabled	"SMS Full Content" User privilege Disabled
Enable	Enable	Original traffic (from short-term archive)	Masked traffic (from long-term or DC archive)
Enable	Disable	Masked traffic (from long-term or DC archive)	Masked traffic (from long-term or DC archive)
Disable	Enable/Disable	Original traffic from the archive configured in S2D profile	Original traffic from the archive configured in S2D profile

Media Configuration Tab

The G10 Comprehensive RTP Media Capture feature is a licensable feature and is enabled and controlled by a Tektronix Communications Engineer. Once enabled, you can only view the settings. Contact Tektronix Communications for assistance with enabling this feature and configuring these settings.

A separate license is required to playback the RTP streams captured using this feature. This feature is only supported on specific probe configurations.

The G10 Comprehensive Media Capture feature provides the capability to capture ALL RTP media streams on per-probe basis. All captured media is available for analysis and playback in ISA using the Analyze Media feature. Refer to the Iris online help for ISA details.

Comprehensive RTP Media Capture

Voice RTP	Tektronix Communications engineers enable or disable capture of voice, video, or other (RTP traffic not classified as video or voice) packets. • All - unlimited capture; all packets from the stream are captured. • Only First - limited capture; define the number of packets in an RTP stream you want to capture. Valid range is 250-200000 packets.
Video RTP	
Other RTP	
Save	Save all current settings.
Cancel	Cancel changes.

G10 Probe Support

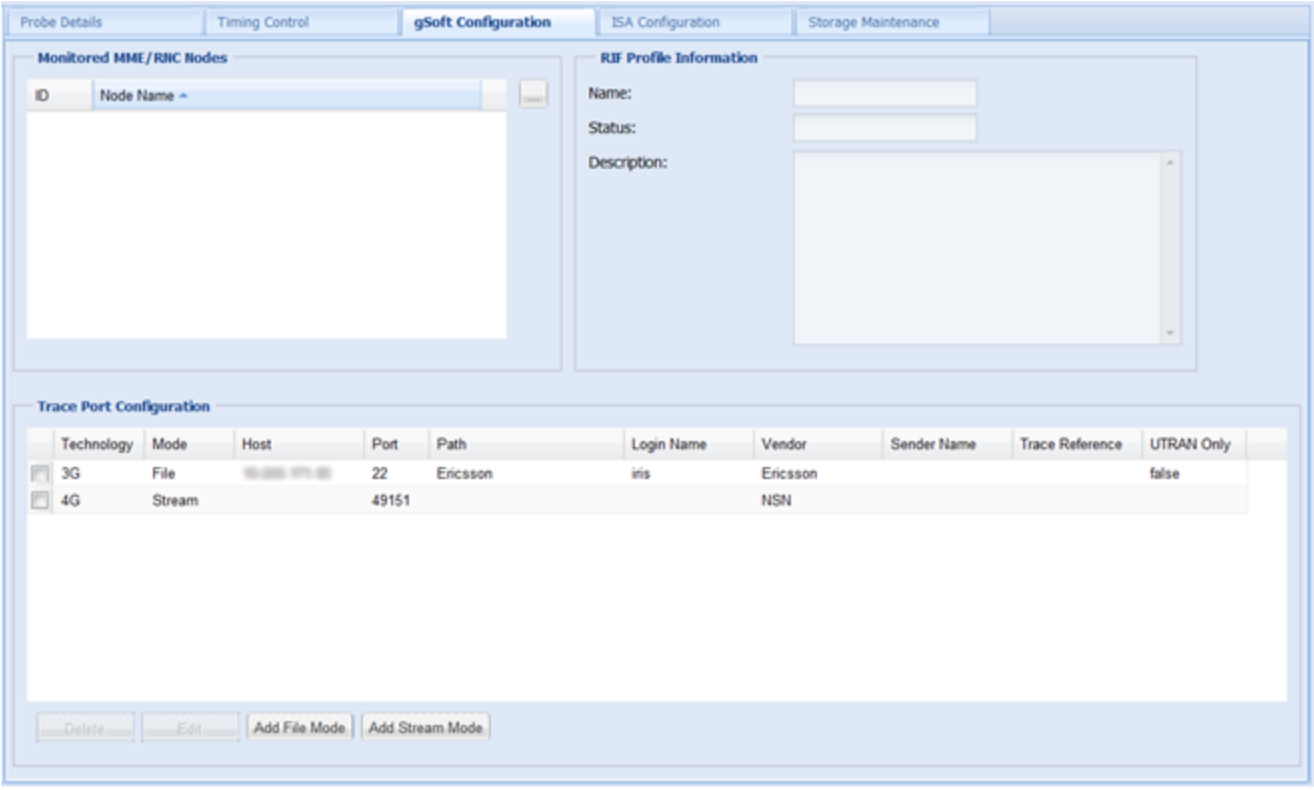
The G10 Media Probe requires special SAS cabling to support the Comprehensive RTP Media Capture feature. Refer to the Media Probe Installation Guide for more details.

Probe Variant	IIC type	IAP type	Storage Array (SA) type	Feature Supported?
Standalone G10	IIC100	IAP100	SA100	YES
	IIC100	IAP200/IAP320	SA100	YES
	IIC200	IAP100	SA100	YES
	IIC200	IAP200/IAP320	SA100	YES
	IIC100	IAP100	SA200	YES
	IIC100	IAP200/IAP320	SA200	YES
	IIC200	IAP100	SA200	YES
	IIC200	IAP200/IAP320	SA200	YES
G10 Media Probe with Comprehensive RTP Media Capture DISABLED	IIC100/IIC200	IAP200/IAP320	SA100/SA200	NO
G10 Media Probe with Comprehensive RTP Media Capture ENABLED	IIC200	IAP200/IAP320	SA200	YES
G10 Control Plane Probe	IIC100/IIC200	IAP200/IAP320	SA100/SA200	NO
gSoft RAN Probe	N/A	N/A	N/A	NO
TD140	N/A	N/A	N/A	NO

Media Configuration Tab

gSoft Configuration Tab

The gSoft Configuration tab enables you to configure probes settings for the GeoSoft RAN probe as described in the Configuring GeoSoft RAN Probes topic.



Monitored MME/RNC Nodes Area

ID	An internal identifier used by the Iris server. The ID is assigned in the order of MME or RNC registration with the server. The first MME/RNC registered uses ID 1, the subsequent one is assigned ID 2, etc.
Node Name	The name that has been defined by the user.
... button	Press this button to open the Select monitored MME/RNC Nodes dialog box to select which MME or RNC is to be monitored.

RIF Profile Information Area

The RIF Profile Information area provides read-only information and is not configurable here. It indicates if the RAN Intelligence Feed (RIF) function is configured for the selected GeoSoft RAN probe and if so, name, status, and description of the configured RIF.

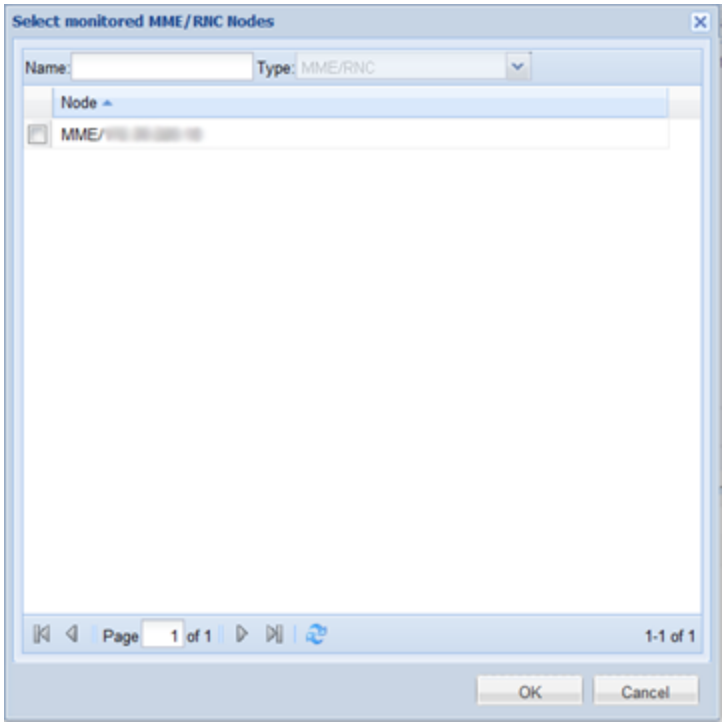
Trace Port Configuration Area

In the eNB Trace Port Configuration area, configure the trace ports to be monitored.

Check Box Column	Click the check box to activate the appropriate technology and mode for your measurement:
Technology	• **3G**: Third Generation - cell phone technologies covered by the ITU IMT-2000 family. • **4G**: Fourth Generation - cell phone technologies covered by the ITU IMT-2000 family.
Mode	• **File**: The file mode applies for vendors, such as Huawei, Alcatel Lucent, and Ericsson, who provide the TCE data for download in form of zip files. • **Stream**: The stream mode applies for vendors, such as NSN, who send the TCE data to the gSoft probe via a TCP connection.
Host (File Mode only)	Lists the IP address or DNS name of the SFTP server.
Port	• **File Mode**: Port of the configured SFTP site • **Stream Mode**: TCP Port to be opened by the gSoft probe
Path (File Mode only)	Path to the root directory of the SFTP server.
Login Name (File Mode only)	Name of an existing user account.
Vendor	Vendor name.
Sender Name	Vendor-provided string for the eNodeB that generates the trace data.
UTRAN Only	Indicates that Iu messages are processed to extract digits for correlation only. RANAP Iu messages and transactions are not associated to the session record.
Trace Reference	The Trace Reference is an ID administrated via the eNodeB's O&M interface to identify a specific trace configuration inside the eNodeB.
Delete	Delete a selected configuration.
Edit	Edit a selected configuration.
Add File Mode	Add a new file mode configuration. The Add File Mode dialog box opens (see Configuring GeoSoft RAN Probes).
Add Stream Mode	Add a new stream mode configuration. The Stream Mode dialog box opens (see the Configuring GeoSoft RAN Probes).

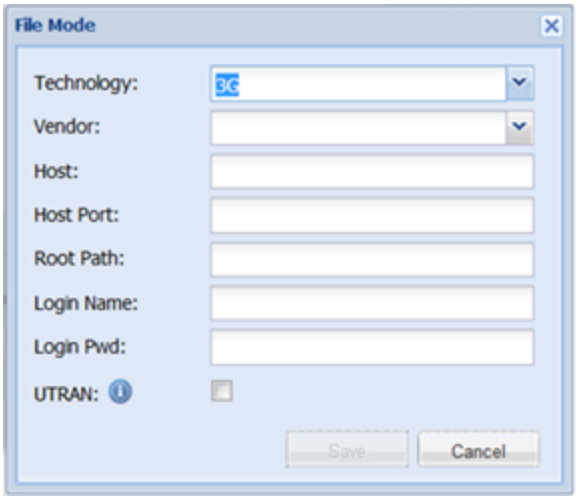
Select Monitored MMEs/RNC Nodes Dialog Box

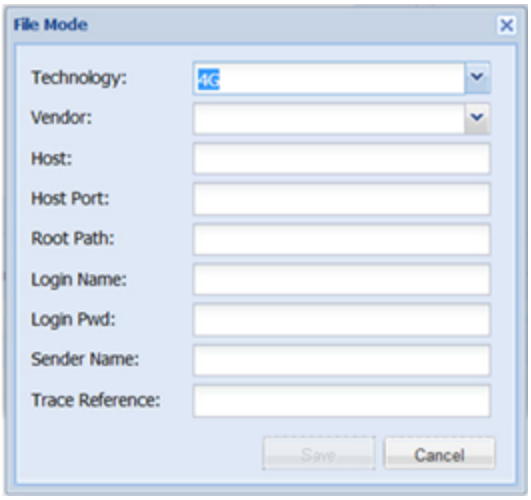
In this dialog box, you can search and sort all available MMEs and RNCs. To search for an MME or RNC, enter your query in the Name field and press OK. To select MMEs/RNCs for your measurement, select the check box on the left-hand side of the Node column.



File Mode Dialog Box

The following figures show File Mode dialog boxes for 3G and 4G trace port configurations.



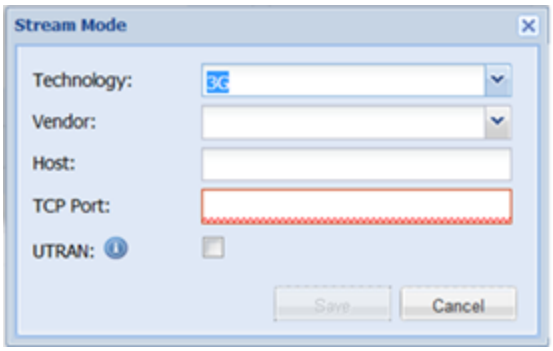


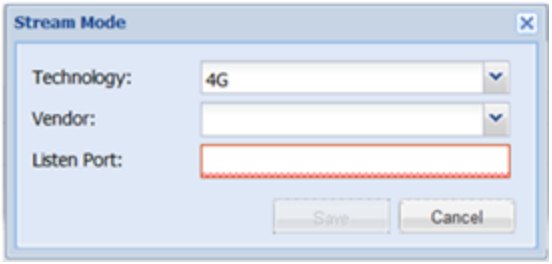
Technology	Select **3G** or **4G** from the Technology drop down list.
Vendor	Select **Huawei**, **ALU**, or **Ericsson** from the Vendor drop down list.

Host	Enter the IP address or DNS name of the SFTP server.
Host Port	Enter the port of the configured SFTP site.
Root Path	Enter the path to the root directory of the SFTP server. That is the place where IRIS starts searching for trace port files.
Login Name	Enter a login name of an existing user account.
Login Pwd	Enter the password for the defined login name.
UTRAN	3G only. Select this check box to process the Iu messages to extract digits for correlation only. Thus, RANAP Iu messages and transactions are not associated to the session record.
Sender Name	Enter a vendor given string for the eNodeB that generates the trace data.
Trace Reference	4G only. The Trace Reference is an ID administrated via the eNodeB's O&M interface to identify a specific trace configuration inside the eNodeB. **Note:**Sender Name **and** Trace Reference **are used to build file and folder names on the file server. String matching patterns may be used to limit the data that is retrieved from the file server by this virtual probe. Two probes that are connected to the same SFTP server and use the same patterns (or overlapping patterns, e.g. * for everything) will download and process the same data.**

Stream Mode Dialog Box

The following figures show Stream Mode dialog boxes for 3G and 4G traceport configurations.





Technology	Select **3G** or **4G** from the Technology drop down list.
Vendor	Select **Huawei**, **ALU**, or **Ericsson** from the Vendor drop down list.
Host	Enter the IP address or DNS name of the SFTP server.
TCP Port	Enter the TCP port number of the SFTP server.
UTRAN	3G only. Select this check box to process the Iu messages to extract digits for correlation only. Thus, RANAP Iu messages and transactions are not associated to the session record.
Listen Port	Enter the number of the TCP listener port into the Listen Port field.

ISA Configuration Tab

The ISA Configuration tab is reserved for Tektronix technical support. DO NOT change the ISA Configuration settings, as this can result in loss of data or system degradation.

Storage Maintenance Tab

The Storage Maintenance tab is reserved for Tektronix technical support. See Storage Array Configuration for details. Do not change the Storage Maintenance settings, as this can result in loss of data or system configuration.

TD140 Ports Tab

The TD140 Ports Tab enables you to view and modify ingress and egress port settings for the TD140. There is one panel for ingress and one for egress ports. Ports are designated as shown in TD140 Ports tab. See Ports on TD140 Chassis for a diagram of port locations on the TD140 chassis. Refer to TD140 Configuration Workflow for details.

Ingress Ports Pane

Ingress refers to the ports on which data from the network is entering the TD140.

ID Column	An internal identifier used by the Iris server.
Name Column	The default name is in <slot-port> format. Ports are designated as shown in TD140 Ports tab.
Direction Column	Set the proper direction for each port: RX, TX, or Span (bidirectional). These settings depend on whether the monitored network physically connects to the TD140 via span/mirror ports or optical splitters. • **Optical Tap/Splitter Ports:** these connections can only monitor in one direction, so **RX** or **TX** are valid options. • **Span/Mirror Ports:** these connections can monitor in any direction, so **RX**, **TX**, or **Span** are valid options.
Gb Column	The capacity of the link rate, which can be 1 Gbps or 10 Gbps.
Enabled Column	Enable or disable the link for monitoring. Initially this column has a "true" value (port Enabled). When you click on it, the text is replaced by a checkmark. Clear the checkmark to set the port to "false" (port Disabled).
TX Enabled	Enable or disable light transmission from the TX port. Set this field based on whether the ports are physically configured to support span ports or tap ports. • **Span Ports**: TXEnabled=**TRUE**. Span ports require the TD140 transmit light from the TX port to keep the port active. • **Tap Ports**: TXEnabled=**FALSE**. Tap ports do not use the TX port and you can disable it.
Op Mode	Select one of the following options for 1G ports. Op Mode is disabled for 10G ports: • **Negotiate** - enables this port to auto-negotiate speed and duplex abilities with client-side ports. • **Full-duplex** - enables communication in both directions, simultaneously. • **Half-duplex** - enables communication in both directions, but only one direction at a time. Set this field based on whether the 1G port is physically configured to support span ports or tap ports. Refer to Physical Device Port Configuration Examples for more information. • **1G Span Ports**: Op Mode=Negotiate; select Full Duplex or Half Duplex only if the monitored equipment is not configured to auto-negotiate. • **1G Tap Ports**: Op Mode=Full Duplex is recommended for most configurations; Half Duplex may be required in certain configurations.
Member Of Column	View the physical link that maps to this port, if any. This field is auto-populated when you configure physical links on the Topology Tab; you cannot modify it. See Configuring Physical Links for details.
Save Button	Save all current TD140 and device port settings.
Cancel Button	Close without saving changes.

Egress Ports Pane

Egress refers to ports on which packet data updated with metadata is transmitted out of the TD140 to the G10 probes.

ID Column	An internal identifier used by the Iris server.
Name Column	The default name is in <slot-port. format. Ports are designated as shown in TD140 Ports tab.
Gb Column	The capacity of the link rate, which is 10 Gbps only for egress ports.
Linked G10	Select one of the G10s that is bound to the TD140.

TD140 Ports Tab

Port Settings for Td140 4106

Ingress Ports

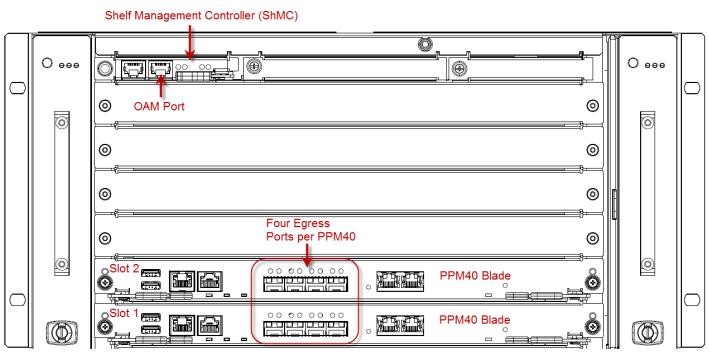
	ID	Name	Direction	Gb	Enabled	TXEnabled	Op Mode	Member Of
PPM40 RTM Slot 1	165	Port 01-09	Tx	10	true	true	Negotiate	TD140_link
	166	Port 01-10	Tx	10	true	true	Negotiate	TD140_link
	167	Port 01-11	Tx	10	true	true	Negotiate	TD140_link
	168	Port 01-12	Tx	10	true	true	Negotiate	TD140_link
	169	Port 01-13	Tx	10	true	true	Negotiate	TD140_link
	170	Port 01-14	Tx	10	true	true	Negotiate	TD140_link
	171	Port 01-15	Tx	10	true	true	Negotiate	TD140_link
	172	Port 01-16	Tx	10	true	true	Negotiate	TD140_link
PPM40 RTM Slot 2	173	Port 02-09	Tx	10	true	true	Negotiate	TD140_link
	174	Port 02-10	Tx	10	true	true	Negotiate	TD140_link
	175	Port 02-11	Tx	10	true	true	Negotiate	TD140_link
	176	Port 02-12	Tx	10	true	true	Negotiate	TD140_link
	177	Port 02-13	Tx	10	true	true	Negotiate	TD140_link
	178	Port 02-14	Tx	10	true	true	Negotiate	TD140_link
	179	Port 02-15	Tx	10	true	true	Negotiate	TD140_link
	180	Port 02-16	Tx	10	true	true	Negotiate	TD140_link

Egress Ports

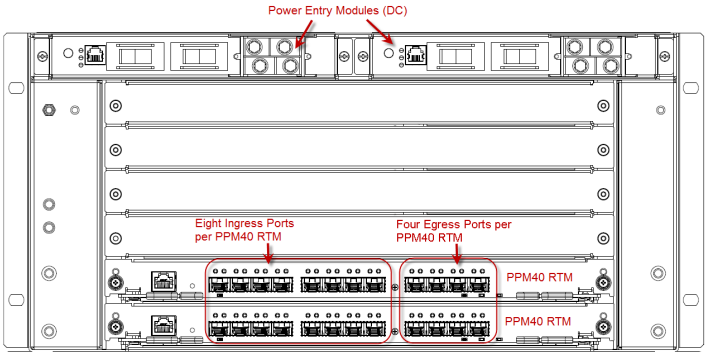
	ID	Name	Gb	Linked G10
Slot 1 PPM40 RTM	145	Port 01-01	10	g309
	148	Port 01-02	10	g313
	150	Port 01-03	10	g313
	152	Port 01-04	10	None
	153	Port 01-05	10	None
	154	Port 01-06	10	None
	155	Port 01-07	10	None
	156	Port 01-08	10	None
Slot 2 PPM40 RTM	157	Port 02-01	10	None
	158	Port 02-02	10	None
	159	Port 02-03	10	None
	160	Port 02-04	10	None
	161	Port 02-05	10	None
	162	Port 02-06	10	None
	163	Port 02-07	10	None
	164	Port 02-08	10	None

Delete TD140 Device | Add to Group | Save | Cancel

TD140 Ports on Chassis



TD140 Front View



TD140 Rear View

TD140 Details Tab

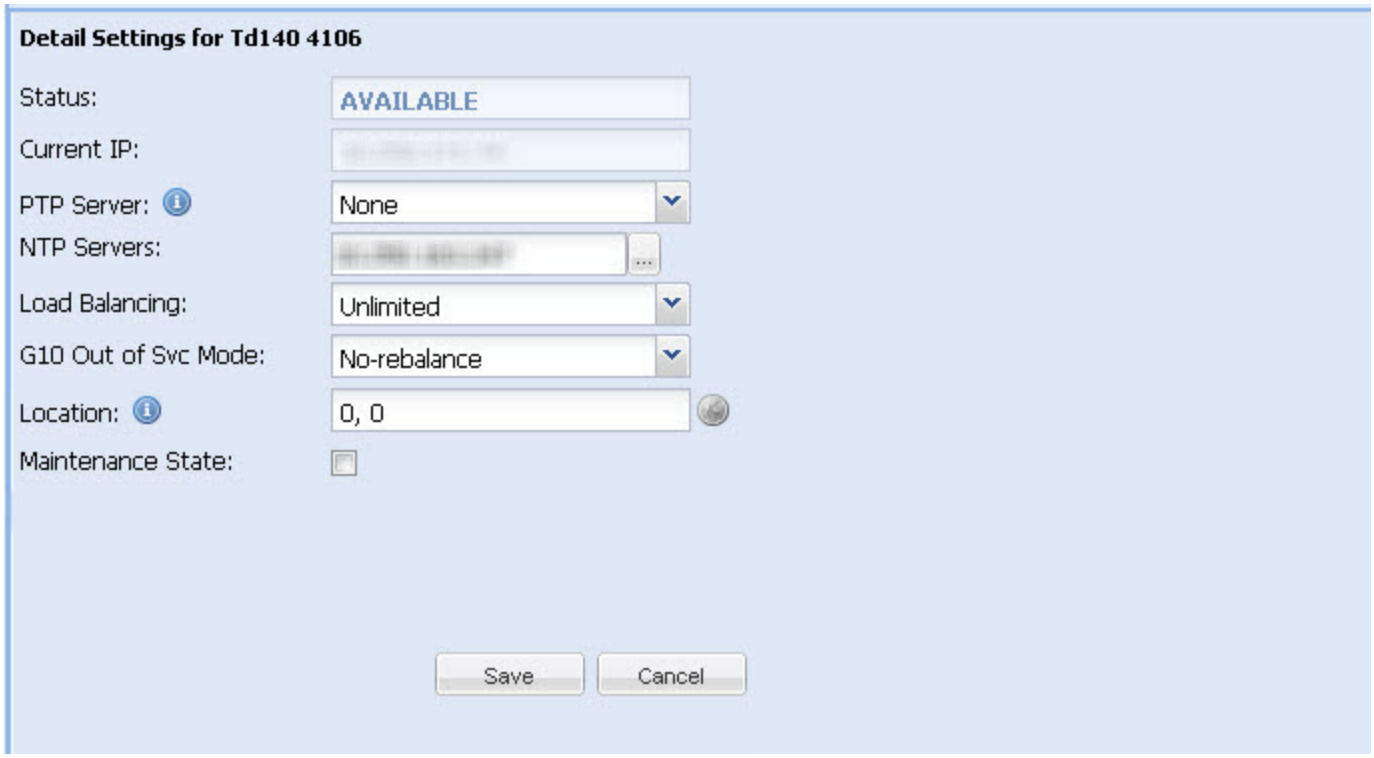
The TD140 Details tab enables you to configure the following properties for the TD140. Refer to TD140 Configuration Workflow for details.

Tektronix Communications System Engineers: Information about the additional configuration fields can be found in the TD140 Technical User Guide.

Status Field	Status field Indicates whether the TD140 is AVAILABLE or in a MAINTENANCE state. When a TD140 is in a maintenance state, system alarms for the probe are not generated
Current IP	View the IP address that was configured on the TD140 at installation. You cannot modify this field.
PTP Server	Enter a single valid IPv4 or IPv6 address to define a PTP server the TD140 will use to synchronize time. You can also select the system-defined PTP server from the drop-down menu. A TD140 can only be assigned one PTP server.
NTP Servers	• The TD140 will select among the listed servers as defined in the NTP v4 specification. • Listing two servers is not recommended; including three or more servers provides the most reliable operation.
Load Balancing	• **Passthrough**: TD140 passes the packets through without any load balancing. • **Unlimited**: New sessions are allocated to the probe with the most available capacity relative to defined session and packet limits. When all probes have exceeded their limits, new sessions are allocated to probes based on a round-robin scheme. There are no packet drops or session aborts at the TD140 when probes are overloaded. • **Limited**: New sessions are allocated to the probe with the most available capacity relative to defined session and packet limits. If all probes are at their maximum capacity, then abort the least recently used session for the new session. If a probe exceeds its configured packet rate session drop onset threshold, then sessions shall be aborted at random until the packet rate drops below the drop onset threshold. New sessions shall be allocated to the probe only after its packet rate drops below a session drop halt threshold. The TD140 tracks aborted sessions caused by probe capacity overruns so that any matching packets can be discarded. Uncorrelated GTP-U packets are discarded.
G10 Out of Svc Mode	• **No rebalance**: In the event of a probe failure, sessions are NOT re-balanced. All traffic destined for the out-of-service probe is dropped. This includes GTPv0, non-GTP, non-IP, and uncorrelated GTP packets. • **Single-rebalancing**: In the event of a single probe failure, sessions are rebalanced to the remaining G10 probes for the first G10 probe that goes out-of-service. Traffic is NOT re-balanced if multiple G10 probes are out-of-service. GTPv0, non-GTP, non-IP, and uncorrelated GTP packets are also re-balanced in this mode.

Location	Enter a city name to search by city or the Latitude and Longitude coordinate for the location you want the element to appear on the map. Various Internet sites provide longitude and latitude coordinates when you enter address information. • Valid latitude coordinates are between -90 and 90 • Valid longitude coordinates are between -179.99 and 179.99 • Lat/Lon values separated by a comma or semi-colon can be copied from a source (such as the Internet) and pasted into either field; Iris automatically separates the values into separate fields • If no coordinates are defined, Iris will assign the default longitude and latitude values set in the Locations Tab. The Location icon indicates how the coordinates were set: • Gray - coordinates set by system based on mapping rules configured in the Locations Tab. The settings will automatically be updated with any changes to the Location rules or you can manually update the coordinates in this pane or directly on the map. • Green - coordinates were manually set; the settings will not be overwritten by updates to the Location rules.
Maintenance State Check Box	Enable/disable a TD140's maintenance status. This check box is only visible to users with the Admin privilege. When a TD140 is in a maintenance state: • System alarms for the TD140 are not generated • Probes bound to the TD140 will also be placed in a maintenance state and alarms for those probes are not generated. See TD140 Configuration Workflow for binding details.

TD140 Details Tab



TD140 Managed Probes Tab

The Managed Probes tab displays the configuration details for the probes managed by a TD140 device. Refer to TD140 Configuration Workflow for details.

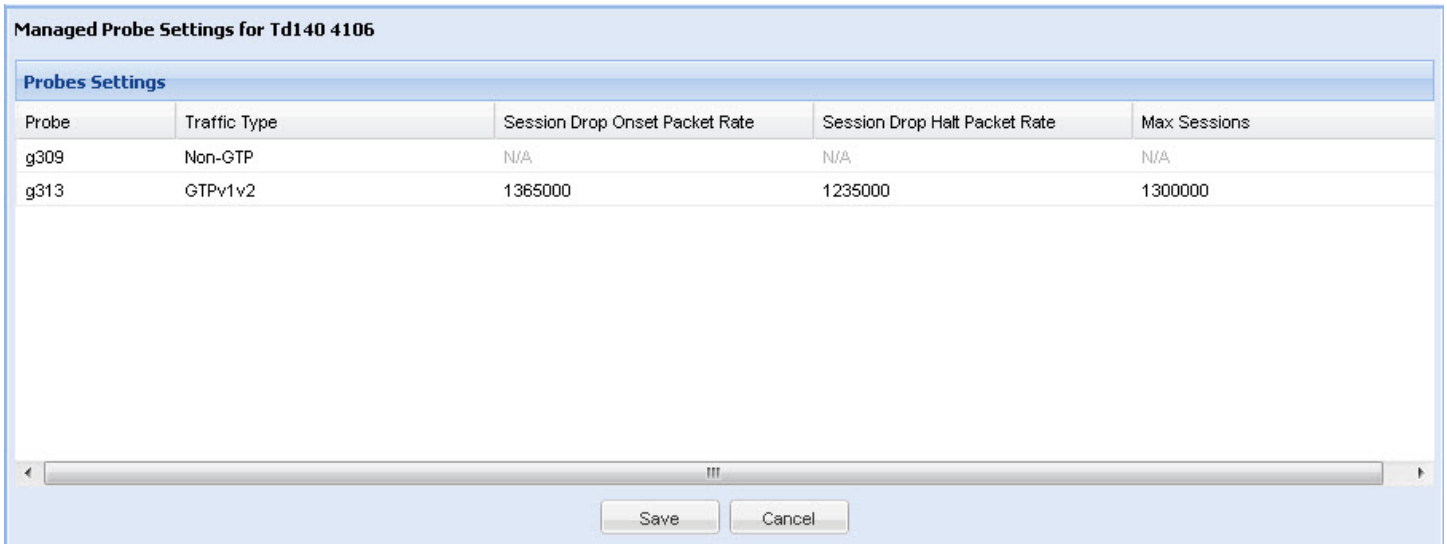
When configuring TD140, the probe capacity limits are set to default values based on each probe's hardware configuration (such as IIC200/IAP200). If a probe's capacity is expected to differ from the default sizing rules, then the per-probe limits must be manually adjusted in IrisView. Examples of things that would affect probe capacity limits are:

- ***DPC enabled***
- ***Full-URL enabled***
- ***Customer traffic model that differs significantly from the standard sizing model***

The following parameters are only applicable when the "Limited" load-balancing scheme is enabled on the TD140 Details tab.

Traffic Type	Configure the type of traffic sent to the selected probe: GtpV1V2, NonGtp, GtpV1V2-NonGtp. Traffic type is initially configured when the probe is first bound to the TD140.
Maximum sessions per G10	Configure the maximum number of session allocations supported for this probe. The default values are determined by installed probe hardware. Users should consider traffic model, features used, as well as probe hardware when determining actual values.
Session drop onset packet rate	Configure the maximum number of packets per second received by a G10 before it starts dropping sessions to accommodate new sessions. The default values are determined by installed probe hardware.
Session drop on halt packet rate	Configure the number of packets received per second a G10 must fall below before sessions resume being allocated to this probe. The default values are determined by installed probe hardware.

TD140 Managed Probes Tab



Software User Interface

Admin contains the following Software GUI elements.

- Software Tab
- By Probe Tab

- Available Patches Tab
- Probe Campaigns Tab
- Campaigns Pane
- Campaign Details Pane
- Firmware Audit Tab

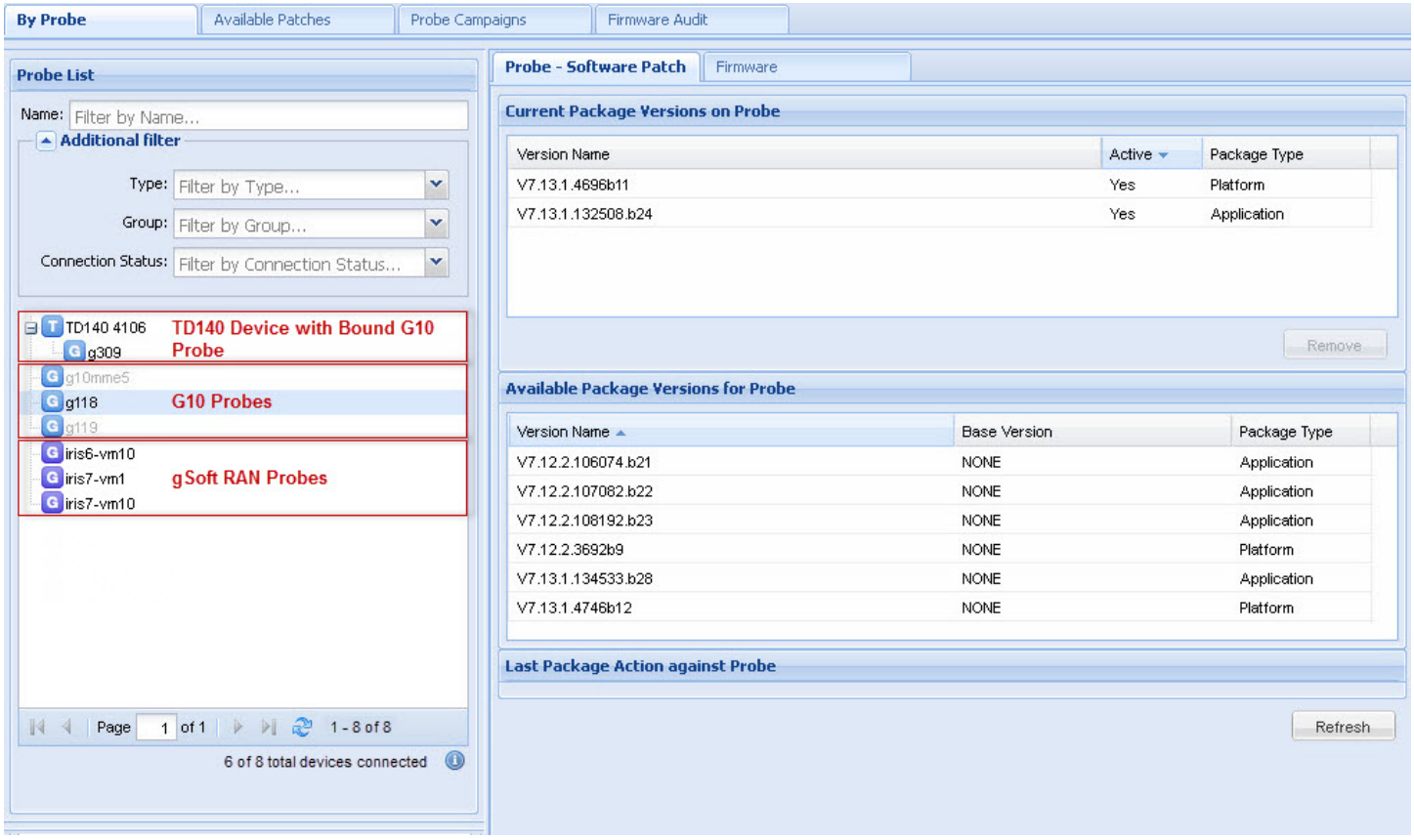
Software Tab

PRIOR TO UPGRADING, YOU MUST READ ALL RELEASE NOTES AND UPGRADE CHECKLISTS TO ENSURE YOU ARE AWARE AND COMPLIANT WITH THE LATEST UPDATES TO THE UPGRADE PROCESS. FAILURE TO COMPLY WITH THE LATEST UPDATES COULD PROLONG THE PROBE UPGRADE PROCESS AND RESULT IN EXTENDED DOWN TIME. CONTACT CUSTOMER SUPPORT FOR ASSISTANCE.

The Software tab enables you to upgrade software packages for G10 and gSoft RAN probes and TD140 devices as well as view and export G10 firmware inventory.

By Probe Tab	Provides a view of the current software packages loaded on individual probes and also the software packages available for the probes on the Iris server.
Available Patches Tab	Enables you to verify software packages.
Probe Campaigns Tab	Enables you to create a probe campaign for upgrading application and platform software packages.
Firmware Audit Tab	Enables you to view and export G10 firmware inventory for multiple probes.

Software Tab



By Probe Tab

This tab enables you to view current software packages per device and firmware inventory per probe. To view firmware inventory for multiple probes/devices, see the Firmware Audit tab.

Probe List Pane	View all provisioned devices that have communicated with the Iris server: G10, TD140, gSoft RAN probes.
Probe - Software Patches Tab	View the current software packages loaded on individual probes and also the software packages available for the probes on the Iris server.
Firmware Tab	**The Firmware Administration privilege is required to access this tab.** Displays an inventory list of active hardware components and their associated firmware for the selected probe. To view inventory for multiple probes/arrays see the Firmware Audit tab. The audit may take several minutes to display, depending on number of devices, components and disk arrays installed on the probe. See also Upgrading G10 Probe and Array Firmware.

Probe List Pane

Name Filter	Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive. • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Type Filter	Select a probe type to filter the probe list. The available tabs vary depending on probe type.
Group Filter	Select a probe group name to filter the probe list. The drop-down menu lists all entity groups defined on the Groups Tab. Group names display in the format [Group Entity] - [Group Name].
Connection Status	Select a connection status as a filter: **All** • View all provisioned probes; both connected and disconnected. **Not connected - Element name appears in gray text** • Element is not available for configuration or updates. • G10 and gSoft: Indicates **either** the probe SwManager connection or the ConfigServer connection is down. • TD140: Indicates the ConfigServer is down. **Connected - Element name appears in black text** • G10 and gSoft: Indicates **both** the ConfigServer and SwManager are up and running, and connected to the Iris server. • TD140: Indicates the ConfigServer is up and running and connected to the Iris server.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.
Statistical Counter	The counter shows the total number of provisioned devices (G10s, TD140s, gSoft probes) and the number of connected devices. G10s bound to TD140s are also included in the count.

Probe - Software Patch Tab

Version Name Column	The **Current Package Versions on Probe** pane lists all packages that have been uploaded to the selected device and indicates which are active. You can select a software version and remove it from the current device, if it is not active. When removed, it moves from this pane to the Available Package Versions for Probe pane. Refer to Upgrading G10 Probe Software and Upgrading TD140 Software for upgrade details. For G10 upgrades, if the base version still appears in this section (regardless of whether it is active or not), only the EP package needs to be copied into the /Staging area, verified and then uploaded and activated using a probe campaign. ***NOTE: For G10s, platform software packages are comprised of an x64 binary file and a mips binary file. The By Probe tab displays only those platform packages for which both the x64 and mips binary files exist on the probe. Therefore, if either binary file does not exist on the probe for a platform package, you cannot view that package from the By Probe tab. Contact Customer Support if you are having difficulty viewing software packages.***
Active Column	
Remove Button	
Version Name Column	The **Available Package Versions for Probe** pane is view-only and lists all packages that are available on the Iris server to load onto the selected device.
Base Version Column	
Package Type Column	
Refresh Button	The Refresh button refreshes the screen.
Last Package	Action against Probe Indicates the last software maintenance action performed on the selected device (such as package activation or package removal).

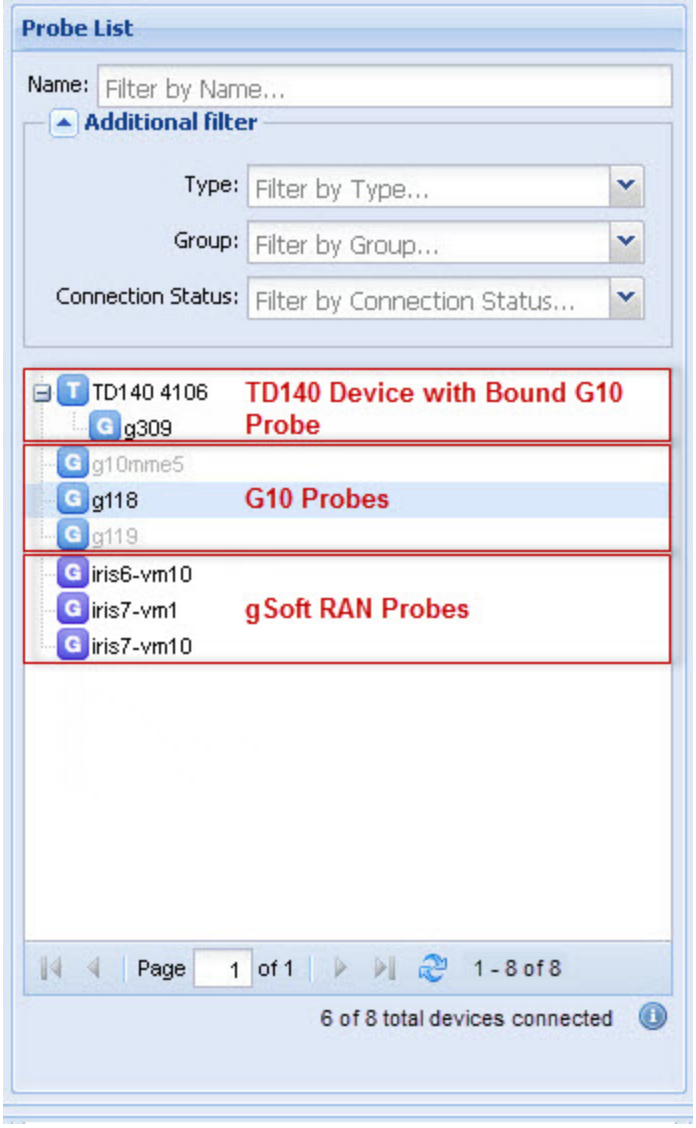
Firmware Tab

You need the Firmware Administration privilege to view this tab. This tab does not apply to TD140 device components; however, you can view firmware inventory for all G10s bound to TD140s.

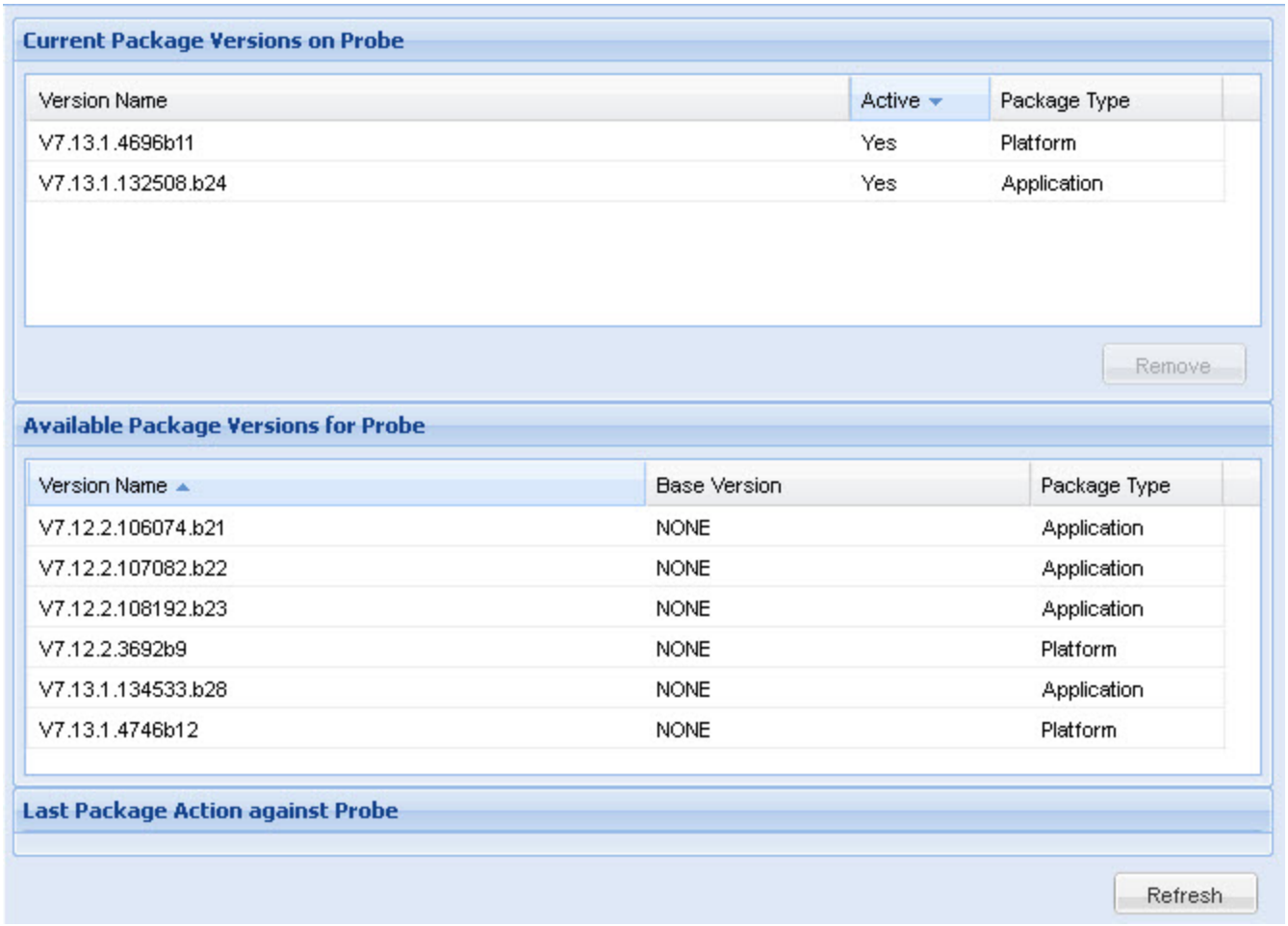
Device column	Lists manufacturer name of blade, SHMM, or storage array. • G10 blades: [Cage.Slot.AMC] • G10 SHMM: Slot letter • Array 0 or 1
Device Location column	
Component column	Designates blade, SHMM, or storage array component and location designated as: • G10 blades: [Cage.Slot] • G10 SHMM: N/A • Storage controllers: [Controller:Module] • Storage disks: [enclosure ID]:[slot ID]
Component Location column	
Active column	Lists the firmware version that is currently running.
Recommended column	Lists the recommended version stored in the current platform software package.
Available column	Lists the firmware versions available for upgrading component (stored in the current platform software package).
Export to CSV button	Open an Export dialog box and select a directory on the Iris server to save the file; the default directory is the Iris server home directory. The file is named using **fw_list_YYYYMMDD_HHMMSS.csv** format.

Refresh Listing button (Firmware Tab only)	Manually refresh the probe inventory. ***Upgrades can fail intermittently causing the firmware listing to be incorrect. Click the Refresh Listing button to ensure the latest firmware information is displayed in the listing. This can take several minutes to complete.***

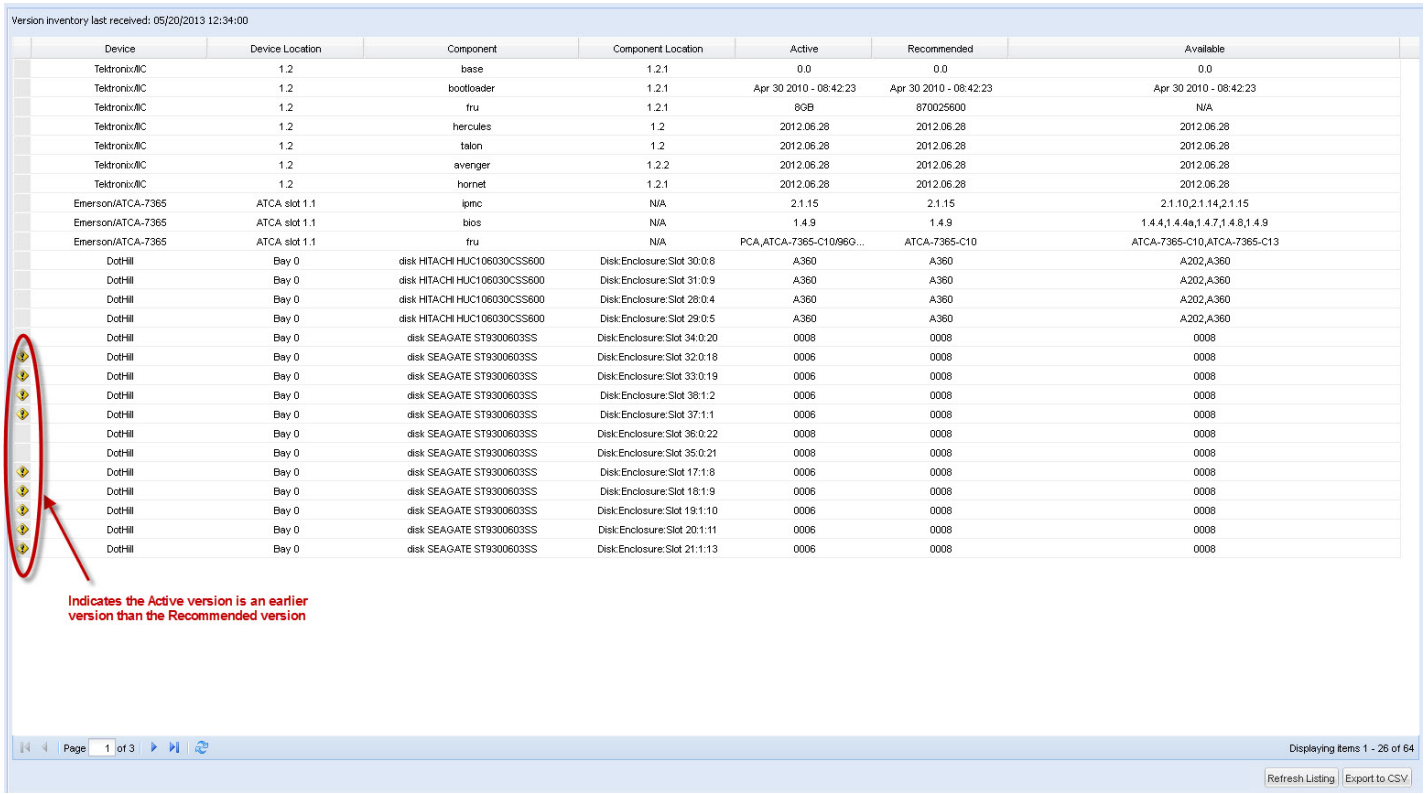
Probe List Pane



Probe - Software Patches Tab



Firmware Tab



Available Patches Tab

The Available Patches tab is used for verifying software packages prior to including them in campaigns for the G10 probe, gSoft RAN probe, and TD140. For workflow details, see the following:

- G10: Upgrading Probe Software or the ***G10 Probe Software Upgrades*** tutorial in the Admin online help.
- gSoft RAN probe: Upgrading Probe Software
- TD140: Upgrading TD140 Software

Probes must have a minimum software version and Emergency Patch (EP) installed to support the version to be upgraded. Contact Customer Support for details.

For EPs requiring base versions, a probe campaign automatically loads the applicable base package with the EP if the base package resides on the Iris Server. You do not need to upload, install, or activate the base version prior to installing the EP. The Base package file (*.pit) must reside on the Iris server and appear in the Available Software Summary pane to be accessible for EP campaigns.

Software List Pane	Provides a list of software files available on the Iris server for installing on probes. Files listed here have not yet been verified.
Available Software Summary Pane	Shows a list of G10 probe software files that have been successfully verified on the Iris server and are available for download to the probe.

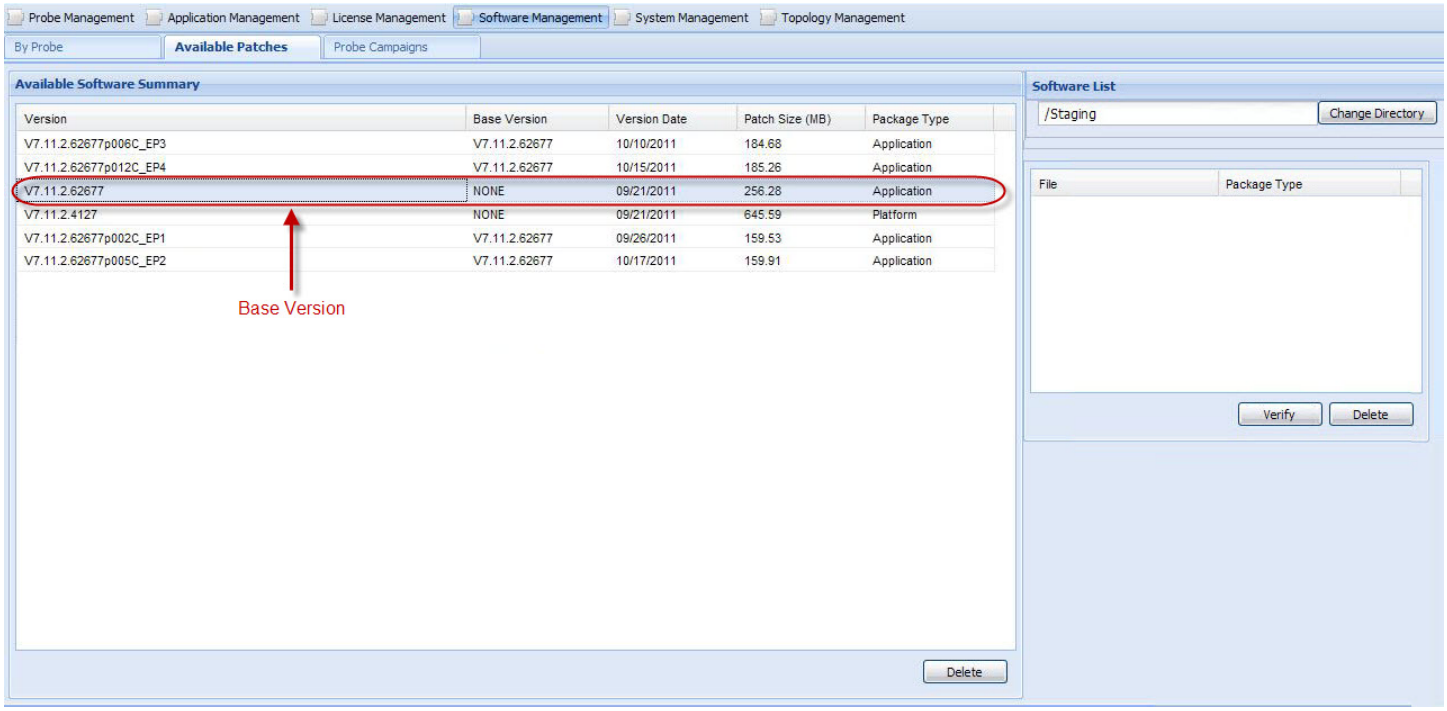
Software List Pane

FTP Folder Field	Tektronix loads software packages in the Iris server /Staging directory.
Change Directory Button	Change the name of the directory if the files have been downloaded elsewhere.
File Column	Lists all files that have been copied to Iris server and made available for installing on probes.
Package Type Column	Indicates package type: • **Application:** Base and EP software package files with a **.pit** extension that contain binaries for various applications that need to be run on the probe • **Platform:** files with **.tgz** extension that contain OS, firmware for the cards, and utilities
Verify Button	Perform a verification test on the selected file to ensure file integrity. • If successful, the package is moved to the Available Software Summary Pane. • If a failure occurs, an error message displays and the file remains in the Software List Pane (contact Customer Support for assistance).
Delete Button	Delete the file from the Iris server, and remove it from the Software List.

Available Software Summary Pane

Version Column	Indicates the version of the G10 probe software file. Files can be either base versions of application or platform software or Emergency Patches (EPs) of application software.
Base Version Column	Identifies the minimum base version required to apply the corresponding patch. "NONE" indicates the package is the base version. For upgrades, if the base version still appears in this section, only the EP package needs to be copied into the /Staging area, verified and then uploaded and activated using a probe campaign.
Version Date Column	Indicates the software file date stamp.
Patch Size (MB) Column	Indicates the software file size.
Package Type Column	Indicates package type: • **Application:** Base and EP software package files with a **.pit** extension that contain binaries for various applications that need to be run on the probe • **Platform:** files with **.tgz** extension that contain OS, firmware for the cards, and utilities
Delete Button	Deletes the file from the Iris server, and removes it from the Available Software Summary pane.

Available Patches Tab



Probe Campaigns Tab

PRIOR TO UPGRADING, YOU MUST READ ALL RELEASE NOTES AND UPGRADE CHECKLISTS TO ENSURE YOU ARE AWARE AND COMPLIANT WITH THE LATEST UPDATES TO THE UPGRADE PROCESS. FAILURE TO COMPLY WITH THE LATEST UPDATES COULD PROLONG THE PROBE UPGRADE PROCESS AND RESULT IN EXTENDED DOWN TIME. CONTACT CUSTOMER SUPPORT FOR ASSISTANCE.

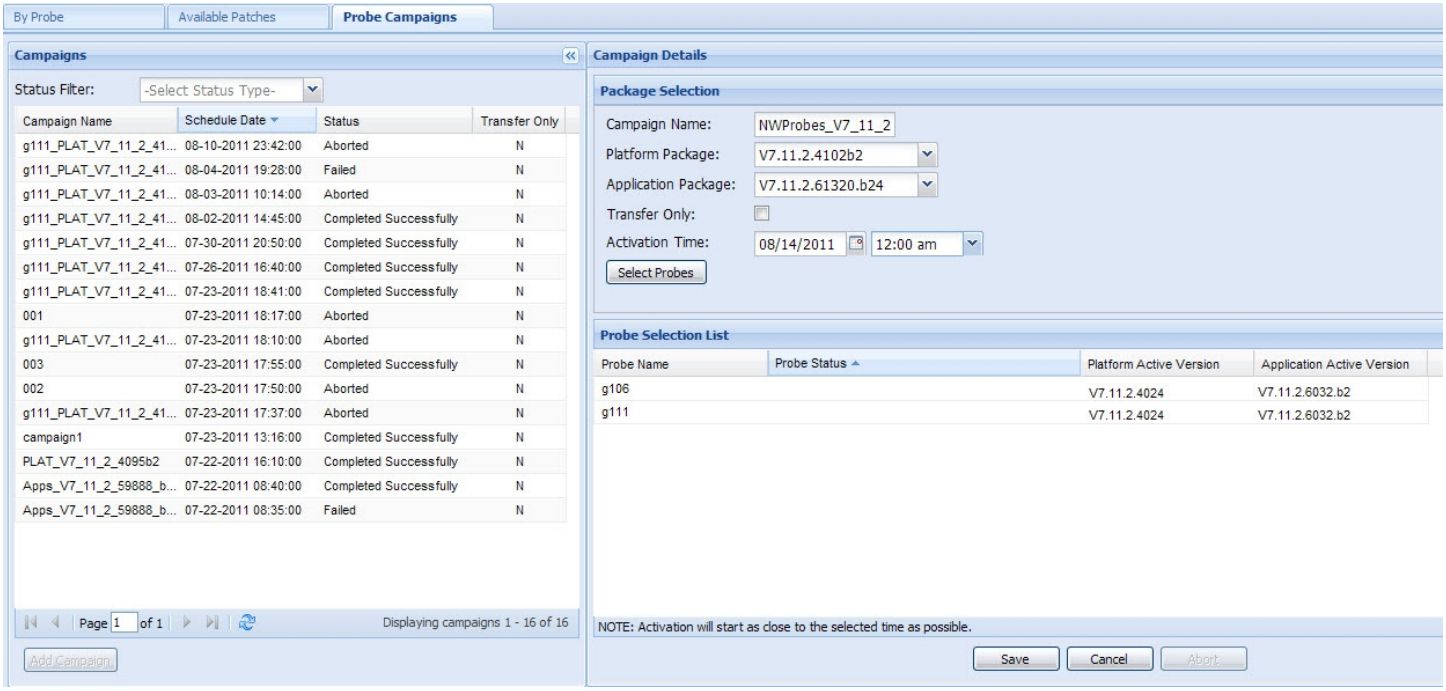
The Probe Campaigns Tab enables you to create campaigns for upgrading software packages for G10 and gSoft RAN probes and TD140 devices as well as G10 probe firmware upgrades. A campaign is a defined set of configuration parameters for upgrading one or more probes or TD140 devices.

You access this window from the Software tab. For workflow details, see the following:

- G10 and gSoft: Upgrading Probe Software
- TD140: Upgrading TD140 Software
- G10 only: Upgrading G10 Probe and Array Firmware

Campaigns Pane	View the status of all existing upgrade campaigns or add a new campaign.
Campaign Details Pane	View the details of existing campaigns or configure the details of new campaigns.

Probe Campaigns Tab



Campaigns Pane

The Campaigns pane enables you to view the status of all existing probe upgrade campaigns and add a new campaign. Select a campaign to view its associated details. Existing campaigns cannot be modified.

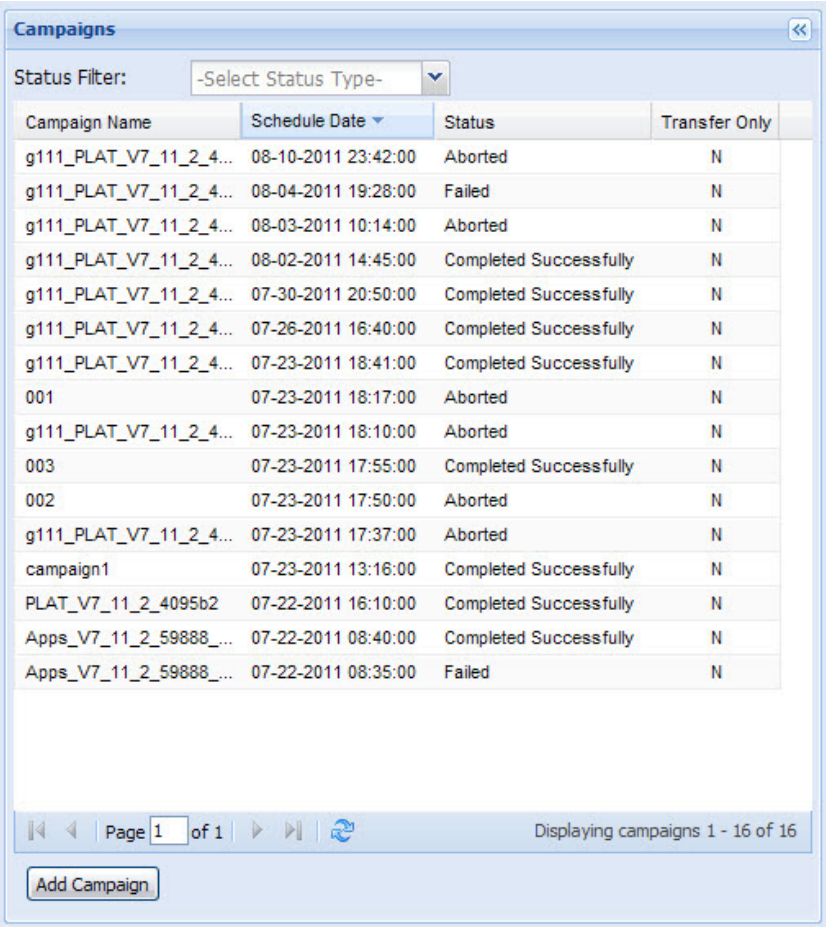
Filter/Paging Controls

Show/Hide Button	Hide or show the Campaigns pane.
Status Filter Drop-Down Menu	Select a campaign status to filter the campaigns table. Select ALL to show all campaigns.
Column Filters	You can apply a sort filter or show or hide columns using an actions menu.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.
Add Campaign	Open the Campaign Details Pane with blank fields for entering new campaign data.

Columns

Campaign Name Column	Lists the names of existing campaigns.
Schedule Date	Shows the date and time activation was scheduled for the campaign. This field is empty for campaigns that were configured to only transfer software packages.
Status	Shows the current campaign status.
Transfer Only	Indicates if the campaign was configured to transfer packages and not activate them.

Campaigns Pane



Campaign Details Pane

PRIOR TO UPGRADING, YOU MUST READ ALL RELEASE NOTES AND UPGRADE CHECKLISTS TO ENSURE YOU ARE AWARE AND COMPLIANT WITH THE LATEST UPDATES TO THE UPGRADE PROCESS. FAILURE TO COMPLY WITH THE LATEST UPDATES COULD PROLONG THE PROBE UPGRADE PROCESS AND RESULT IN EXTENDED DOWN TIME. CONTACT CUSTOMER SUPPORT FOR ASSISTANCE.

The Campaign Details pane enables you to view the configured details of existing campaigns or configure the details of new campaigns.

The fields in the Package Selection Area vary depending on the selected campaign type.

Campaign Type	Select the campaign type you want to create: • G10 - Upgrade probe application and platform software packages. Use this type for gSoft RAN probes. • TD140 - Upgrade TD140 software package • Firmware - Upgrade G10 probe component firmware
Campaign Name Field	Enter a name for the upgrade campaign.

Platform Package Drop-Down Menu Application Package Drop-Down Menu	**Applicable to G10 Campaigns Only** Select a platform or application software package for upgrading probes. Only packages that have been verified (as listed on the Available Patches Tab) are available for selection. ***Probes must have a minimum software version and Emergency Patch (EP) installed to support the version to be upgraded. Contact Customer Support for details.*** ***For EPs requiring base versions, a probe campaign automatically loads the applicable base package with the EP if the base package resides on the Iris Server. You do not need to upload, install, or activate the base version prior to installing the EP. The Base package file (*.pit) must reside on the Iris server and appear in the Available Software Summary pane to be accessible for EP campaigns.***
TD140 Package	**Applicable to TD140 Campaigns Only** Select a TD140 software package. Only packages that have been verified (as listed on the Available Patches Tab) are available for selection.
Select Devices	**Applicable to Firmware Campaigns Only** Click the ellipsis (...) button to open the Select Devices dialog box which contains all devices configured on the selected probes. If a selected group of probes has dissimilar hardware, the list contains all devices for every selected probe. The Save Report indicates which devices are not applicable to certain probes.
Transfer Only Check Box	**Applicable to G10 and TD140 Campaigns Only** Select this option if you do not want the software packages automatically activated on the probe or TD140 once transfer is complete. If you select this option, you must create a new campaign to schedule activation for the probe/TD140.
Activation Date Field Calendar Button Start Time Drop-Down Menu	Select a time to activate software. Tektronix recommends scheduling activation during non-peak hours. The probes require a reboot after activation and this process can take up to 10 minutes. • Enter an activation date by changing the value in the field or by selecting it from a calendar. • To open the calendar, click the Calendar button and then click the date. • Select a future start time (cannot be a time frame that has already expired)
Select Probes	Open the Probe Selector window and select the probes you want to upgrade. Probes are not available to select if the probe is: • disconnected • part of another current campaign • running Store-to-Disk (S2D) configuration ***When scheduling any type of probe campaign (Transfer only, Activation only, and Transfer and Activation), the system administrator can include a maximum of 100 probes in the campaign. See Probe Campaign - Package Transfer and Activation for details about software package transfer and activation.***
Probe Selection List Area (for G10 campaigns)	• Probe name • Probe campaign status • Platform Active version • Application Active version • Managing TD140 (if G10 is bound to a TD140)

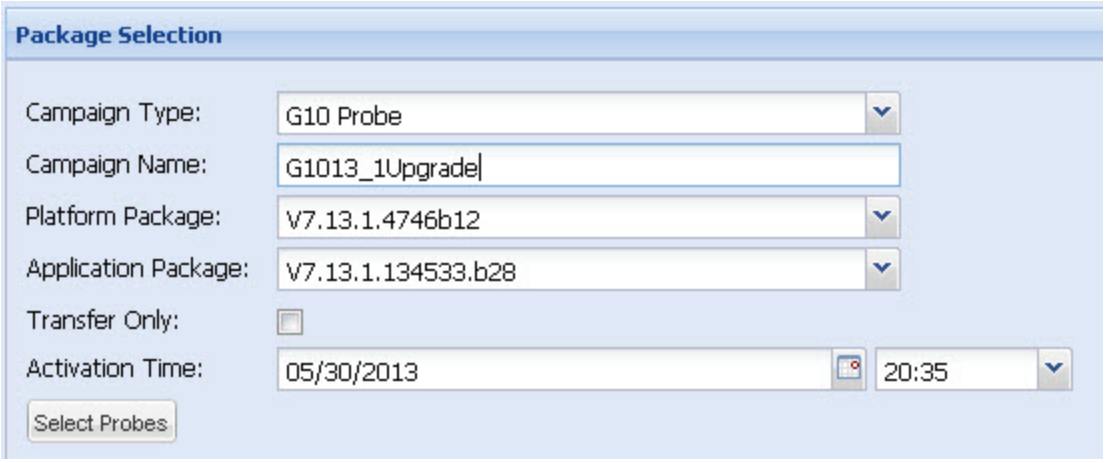
Probe Selection List Area (for TD140 campaigns)	• Probe name • TD140 campaign status • TD140 Active version

Probe Selection List Area (for Firmware campaigns)	• Probe name
	• Probe campaign status; double-click status field to open a Detailed Status Report.
	In some cases, campaign status is reported without a detailed status report:
	• When you select only StorageArray for upgrade and all its components are up-to-date already, campaign will be completed successfully without detailed report with the reason “All storage array components up-to-date”.
	• Campaign failed due to some general problem on probe side. In this case the campaign will be completed with ‘Failed’ status and one of the following reasons:
	  • Server reboot occurred
	  • Firmware manager reported error during upgrade
	  • Firmware validation error
	  • Empty or incorrect firmware report has been received
	• Campaign is aborted before activation.

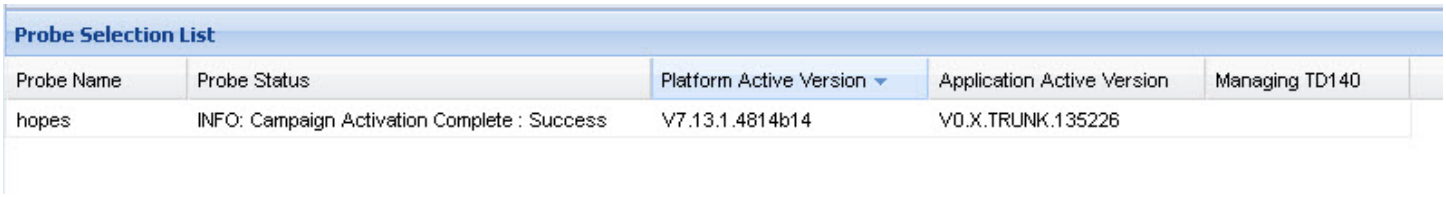
Save Button	**G10 and TD140 Campaigns**: Saves the campaign details and starts the package transfer process. You cannot save a campaign if any of the selected probes in the campaign are currently updating topology. See Probe Campaign - Package Transfer and Activation for details about software package transfer and activation. **Firmware campaigns:** Saves the campaign details and opens the Save Report which indicates the devices that are not applicable to certain probes. The issues reported are informational and are not considered errors.
Cancel Button	Close the Campaign Details Pane without saving changes.
Abort Button	Abort the current campaign. This option is only available when a campaign status is currently *Transferring Packages* or *Activation Scheduled*.
Delete Button	Delete the selected campaign. You can only delete a campaign when it is NOT in one of these states: ACTIVATING, TRANSFERRING_PACKAGES or ACTIVATION_SCHEDULED.

Campaign Details - G10

Package Selection Area - G10

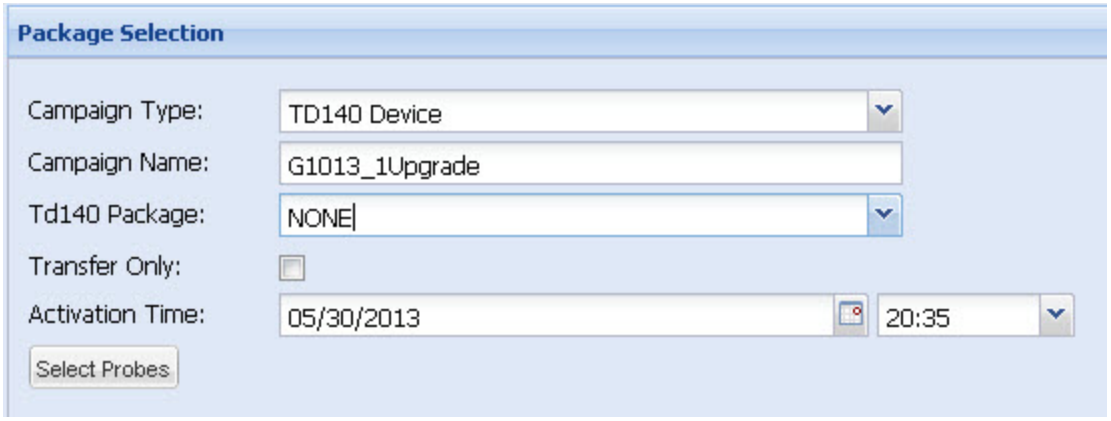


Probe Selection Area - G10

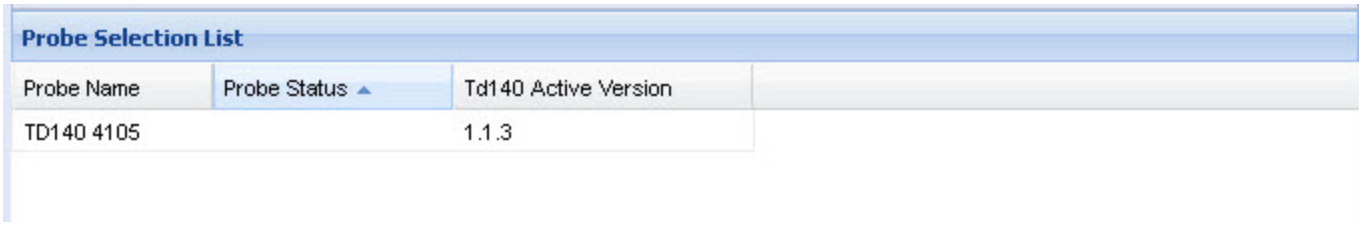


Campaign Details - TD140

Package Selection Area - TD140

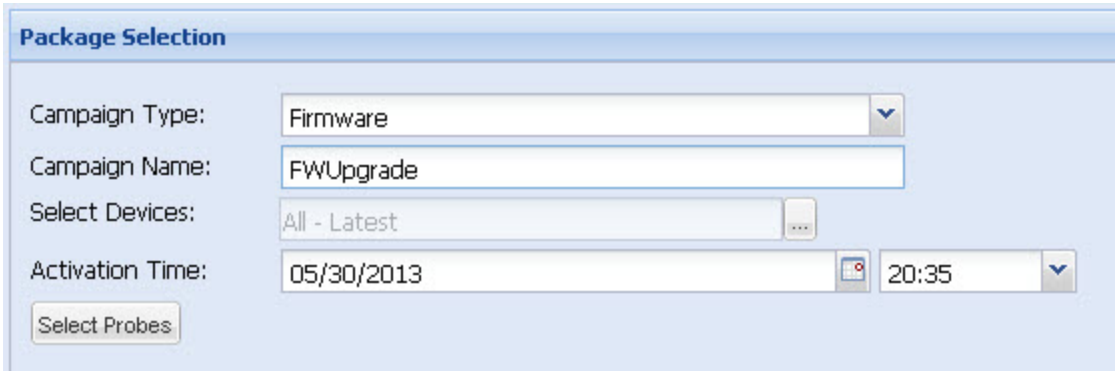


Probe Selection Area - TD140

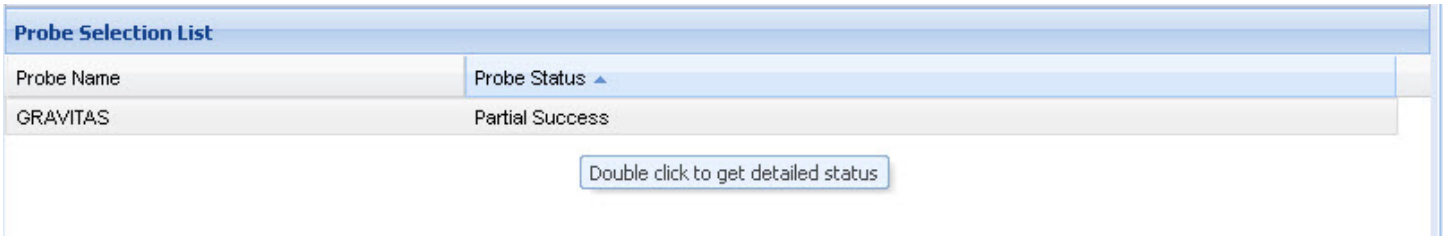


Campaign Details - Firmware

Package Selection Area - Firmware



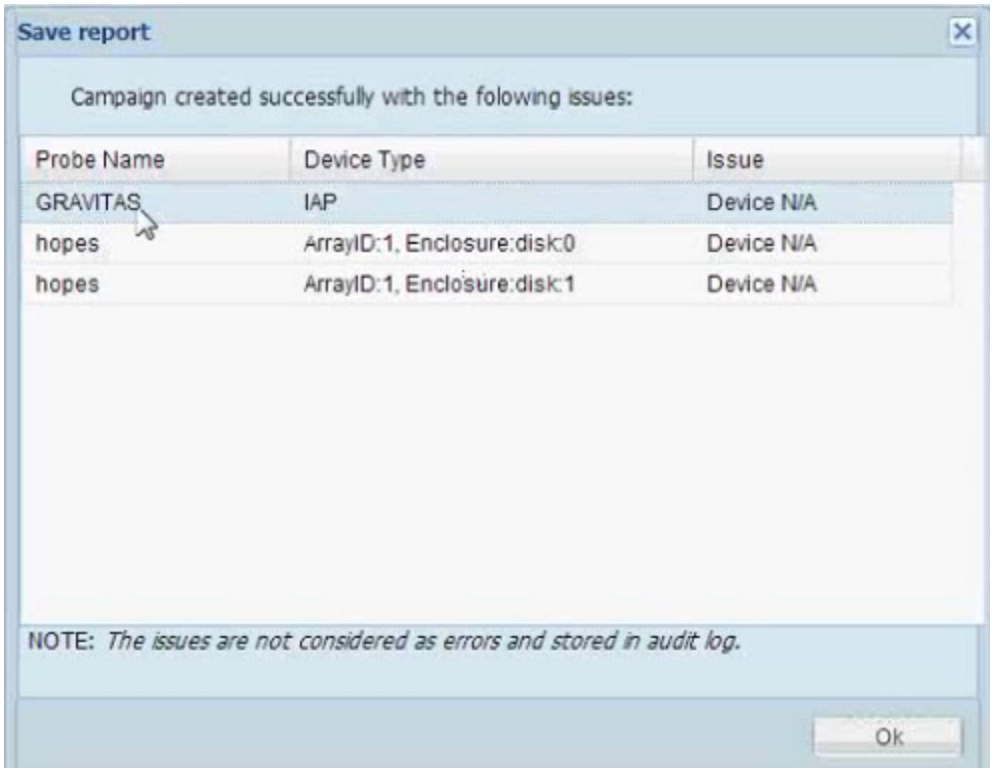
Probe Selection Area - Firmware



Select Devices Dialog Box

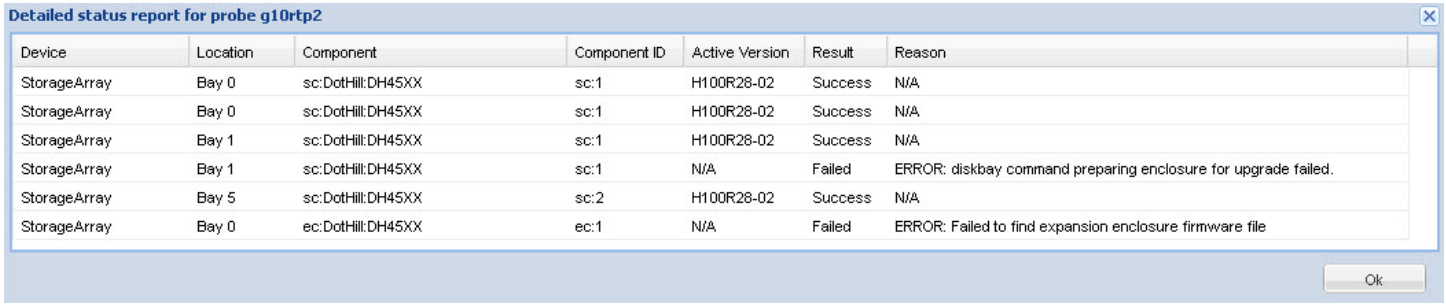
Save Report - Firmware Campaign

This report displays when you save a Firmware campaign that contains multiple probes. It indicates the devices which are not applicable to certain probes.



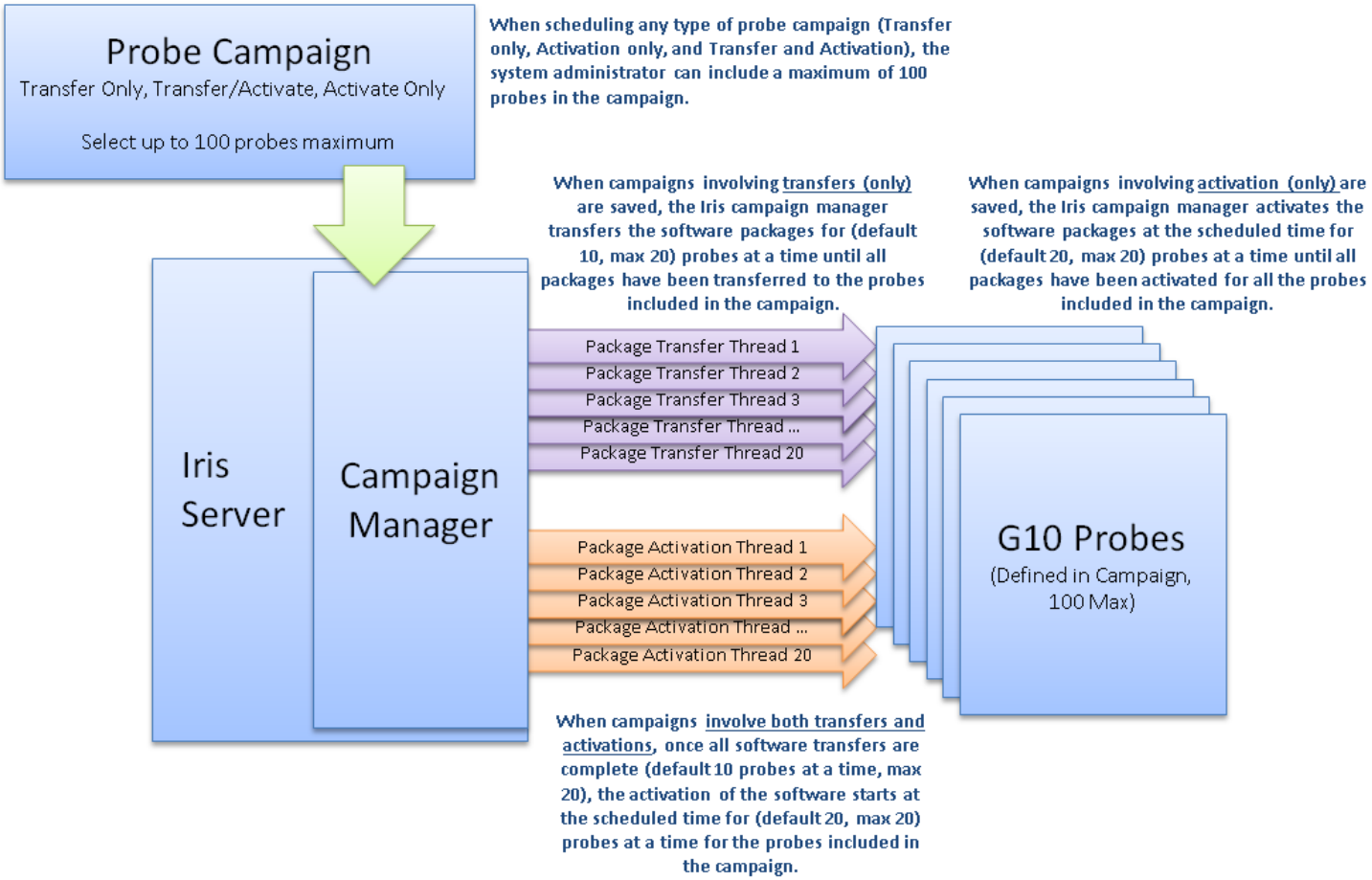
Detailed Status Report - Firmware Campaign

View details about firmware upgrades per component. You access this report by double-clicking the Probe Status field in the Probe Selection area for firmware campaigns.



Probe Campaign - Package Transfer and Activation

The following diagram summarizes the process for transfer and activation of software packages.



Campaign Status

The following campaign status messages appear in the Campaigns Pane.

Transferring Packages	Iris server is transferring packages to one or more probes or TD140s.
Transfer Failed	Transfer of packages failed to one or more probes or TD140s. Review the probe status messages for details.
Activation Scheduled	Transfer of packages was successful to all probes or TD140s. Activation will begin at scheduled time.
Activating	Activation of all probes or TD140s is in process.
Partial Success	One or more probes or TD140s failed package transfer or failed activation. Review the status messages for details.
Completed Successfully	Transfer or activation is complete for all probes or TD140s.
Failed	Transfer or activation failed for all probes or TD140s. Review the status messages for details.
Aborted	User aborted campaign or the probe or TD140 rebooted during the campaign.

Firmware Audit Tab

The Firmware Administration privilege is required to access this tab.

This tab displays an inventory list of all active hardware components and their associated firmware for all connected probes and storage arrays. You can also view per-probe firmware inventory on the By Probe Firmware tab.

The audit may take several minutes to display, depending on number of devices, components and disk arrays installed on the probe. If firmware inventory does not display, it indicates the Iris server has not yet received it from the probe. This could be caused by:

- Firmware audit is still in progress on the probe
- Firmware audit failed on the probe
- Probe is on a software version that does not support firmware audits (minimum of 13.1 software release)

See also Upgrading G10 Probe and Array Firmware.

This tab does not apply to TD140 device components; however, you can view firmware inventory for all G10s bound to TD140s.

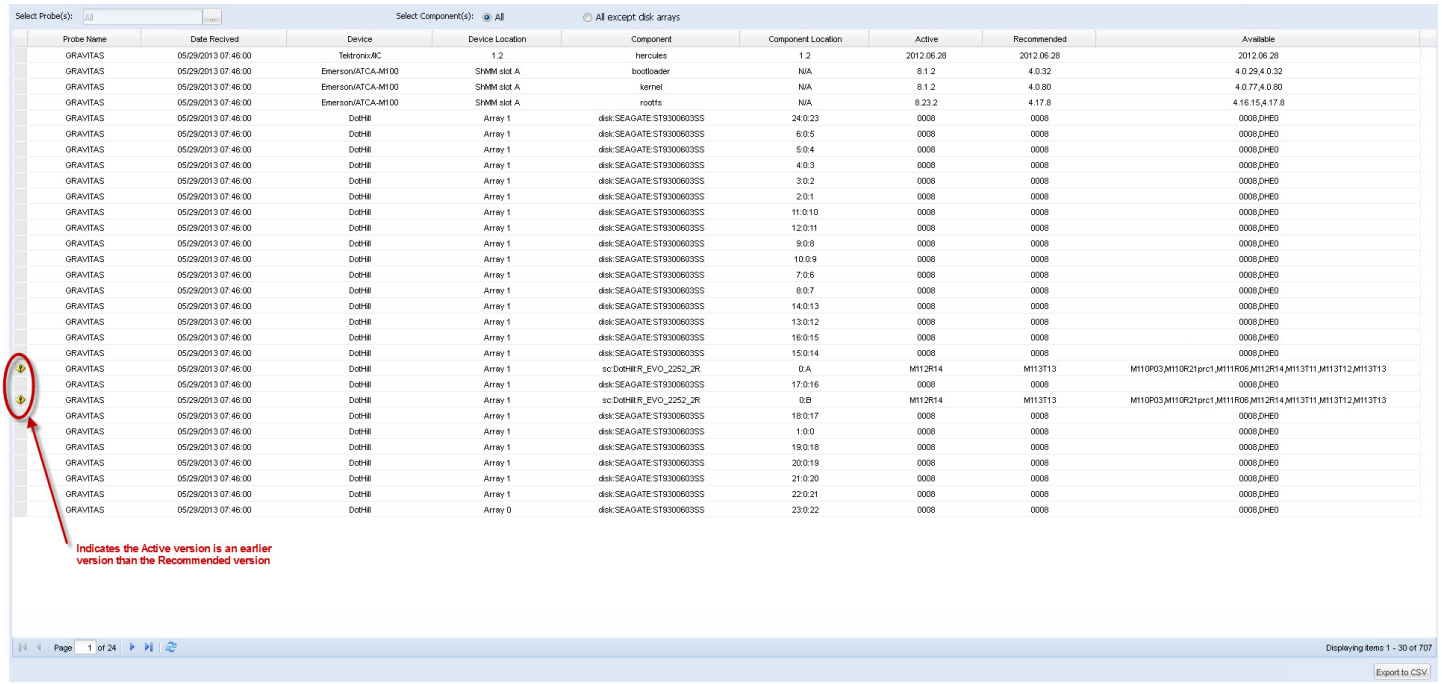
Firmware Audit Tab

Select Probes	Click the ellipsis (...) button to open the Probe Selector dialog box, and select the probes or probe groups you want to view firmware inventory. Selecting a group selects all probes in the group; selecting a TD140 selects all probes bound to the TD140. You can view inventory for disconnected probes. Some probes may have a status of "FW inventory N/A", and cannot be selected. This status could mean: • Firmware audit is still in progress on the probe • Firmware audit failed on the probe • Probe is on a software version that does not support firmware audits (minimum of 13.1 software release)
Select Components Radio Buttons	• **All** - view inventory for all blades, SHMMs, and storage arrays • **All except disk arrays** - hide storage array components
Probe Name Column	Lists the probe name associated with the device/components.
Date Received Column	Lists the date of the last firmware inventory update. This is set when firmware inventory is initially received from probe and is updated with every update of firmware data (such as after a firmware upgrade).

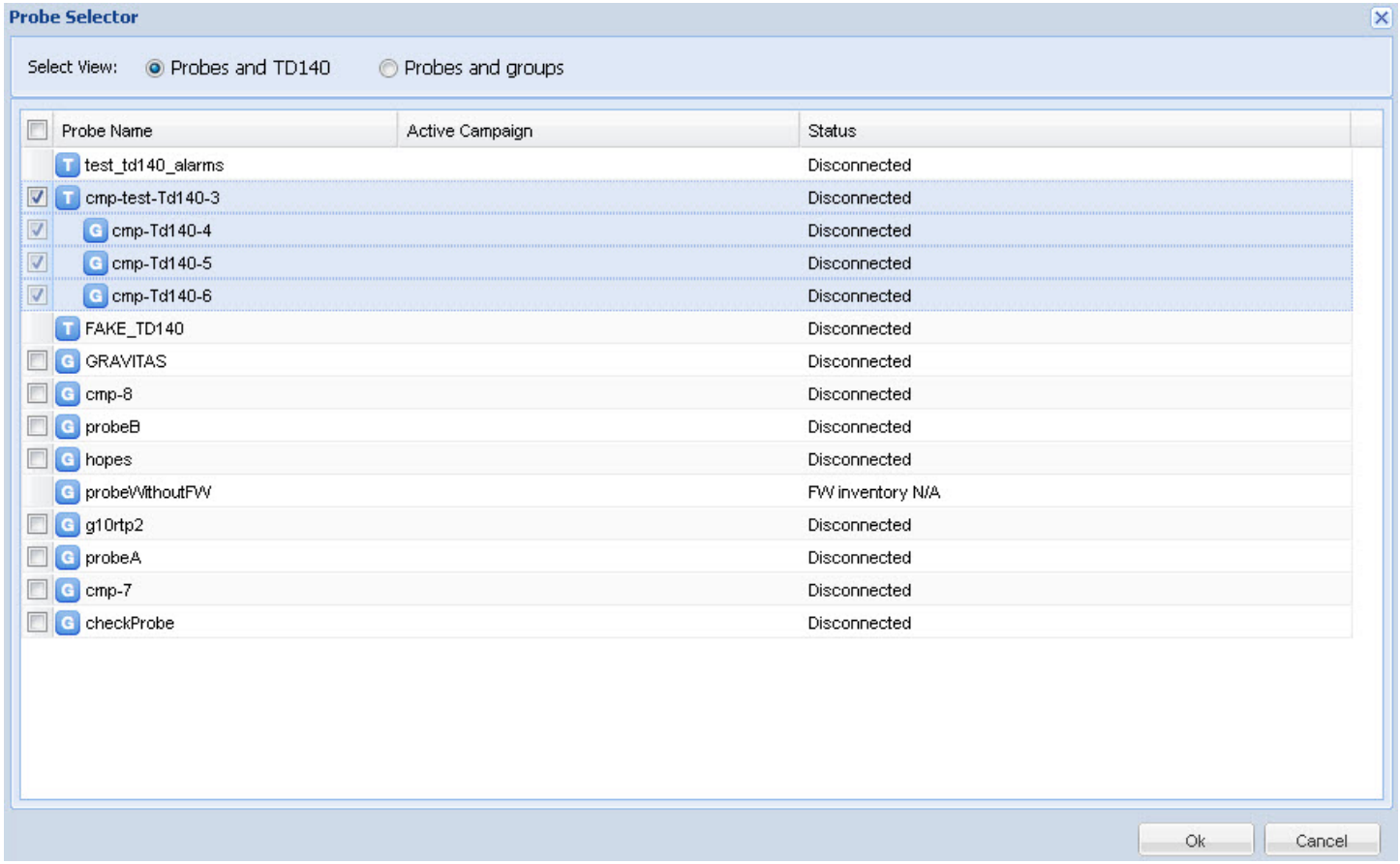
Device column	Lists manufacturer name of blade, SHMM, or storage array. • G10 blades: [Cage.Slot.AMC] • G10 SHMM: Slot letter • Array 0 or 1
Device Location column	
Component column	Designates blade, SHMM, or storage array component and location designated as: • G10 blades: [Cage.Slot] • G10 SHMM: N/A • Storage controllers: [Controller:Module] • Storage disks: [enclosure ID]:[slot ID]
Component Location column	
Active column	Lists the firmware version that is currently running.

Recommended column	Lists the recommended version stored in the current platform software package.
Available column	Lists the firmware versions available for upgrading component (stored in the current platform software package).
Export to CSV button	Open an Export dialog box and select a directory on the Iris server to save the file; the default directory is the Iris server home directory. The file is named using **fw_list_YYYYMMDD_HHMMSS.csv** format.
Refresh Listing button (Firmware Tab only)	Manually refresh the probe inventory. ***Upgrades can fail intermittently causing the firmware listing to be incorrect. Click the Refresh Listing button to ensure the latest firmware information is displayed in the listing. This can take several minutes to complete.***

Firmware Audit Tab



Probe Selector Dialog Box



System User Interface

Admin contains the following System GUI elements.

- System Tab
- Servers Tab
- Config Import Tab
- Config Export Tab

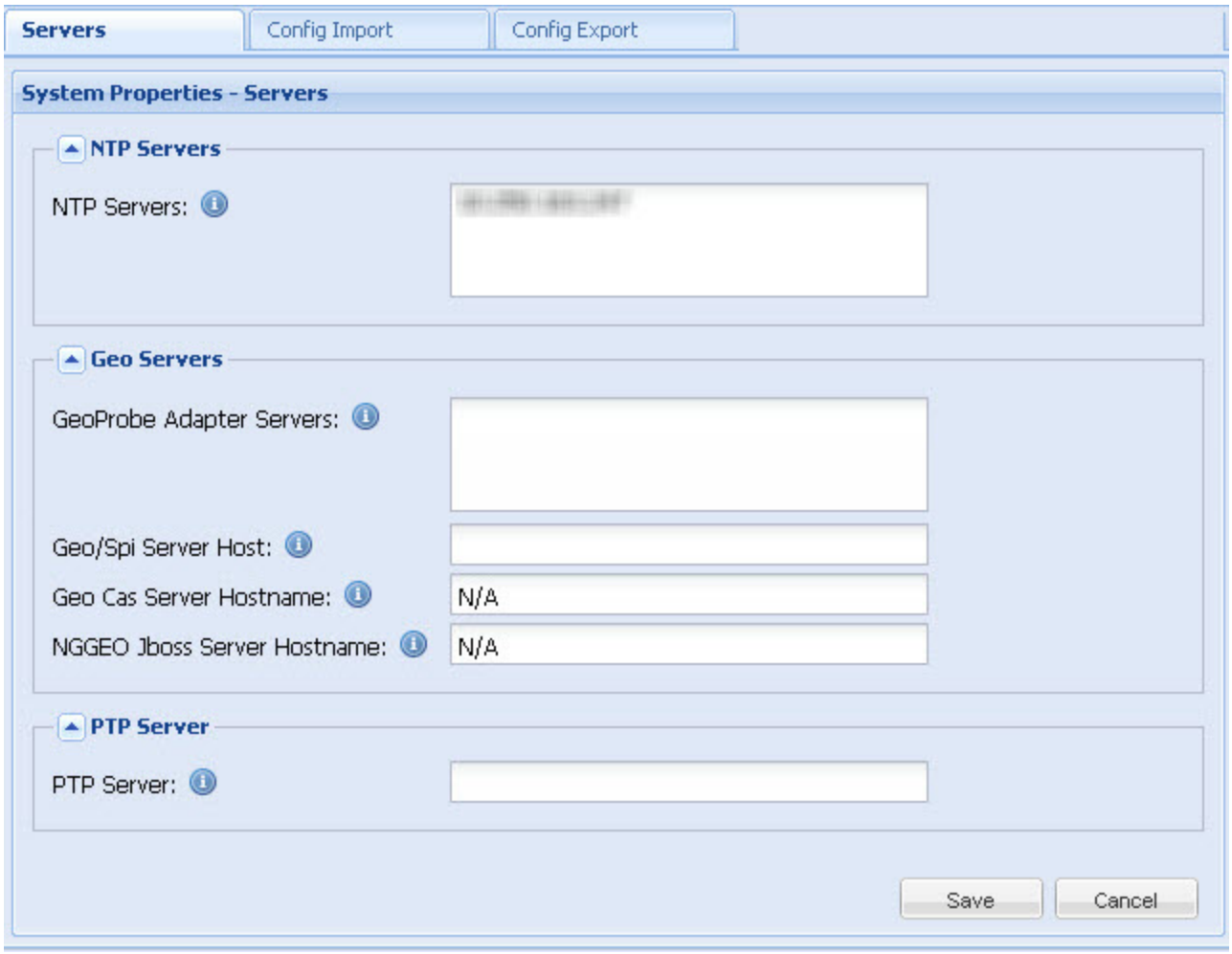
System Tab

The System tab provides the Server configuration tab and tabs for bulk CSV import/exports.

System Tabs

Servers Tab	Define the servers to which the Iris server needs to communicate.
Config Import Tab	Import data from one or more CSV-formatted files for nodes and applications. See Using CSV File Import/Export for details.
Config Export Tab	Export all currently configured information for nodes, protocols, or applications into a CSV-formatted file. See Using CSV File Import/Export for details.

System Tab



Servers Tab

The Servers tab enables you to define the IP addresses and host names for servers to which the Iris server needs to communicate. You access this tab from the System tab.

NTP Servers Area

The G10 probes time stamp all captured messages, generated alarms, and events to a common time base, allowing the Iris system to provide detailed, network-wide traces and event occurrence reporting. Inter-node timing and message paths can also be analyzed throughout the network. The Iris system requires a synchronized time stamp between the GeoProbe G10s and other elements in the system. G10s also support IRIG Timing. Refer to G10 Timing for details.

NTP Servers Field	Enter up to 11 valid IPv4 or IPv6 addresses, separated by commas, to define NTP servers the G10 probes will use to synchronize time from a central location. Addresses defined here can be customized per probe on the Timing Control Tab. G10 probes select the best available NTP server from the list and use it as their timing reference.

Geo Servers Area

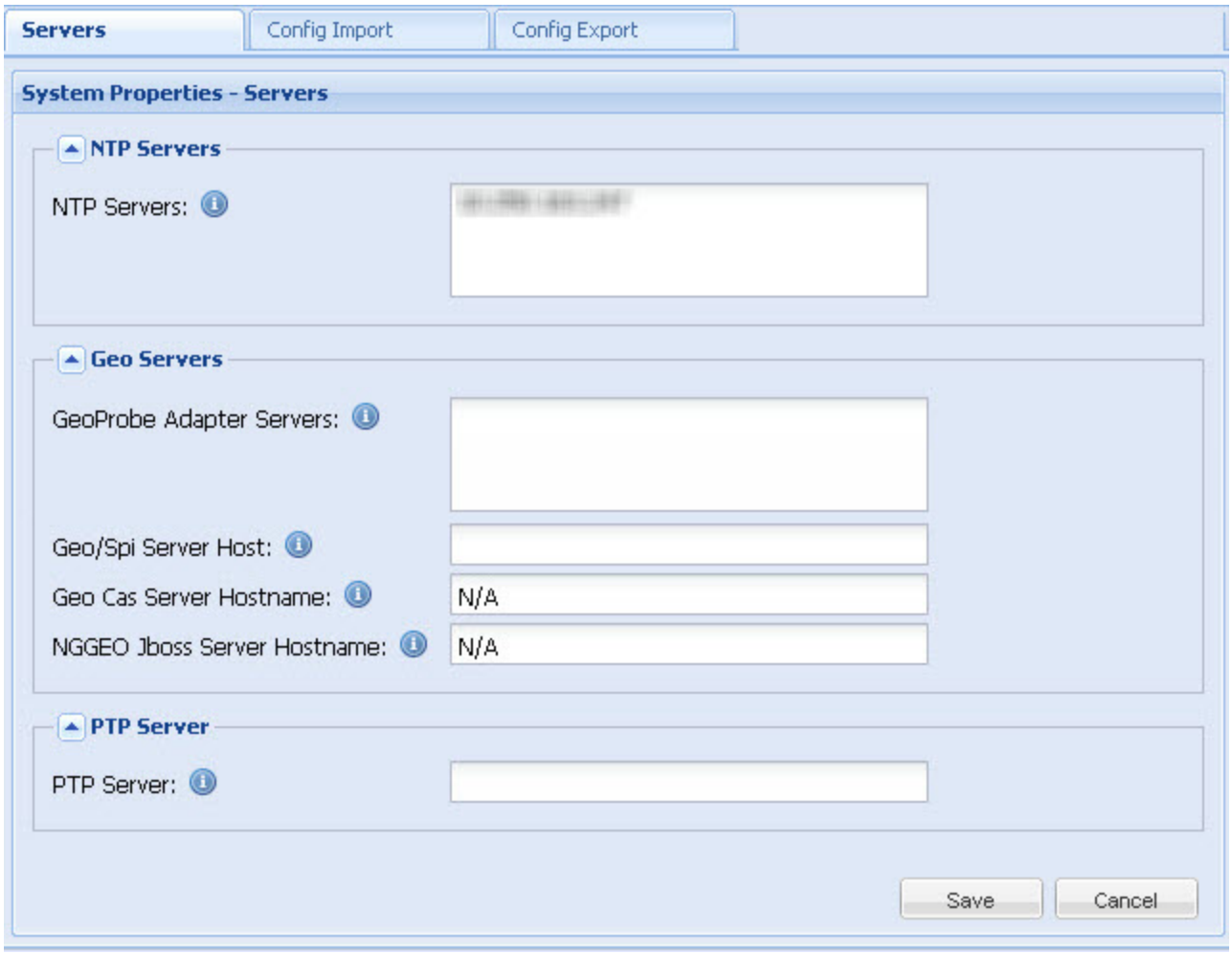
Define IP addresses for the GeoProbe servers supporting Iris.

GeoProbe Adapter Servers Field	Enter multiple IPv4 or IPv6 addresses, separated by commas, corresponding to SpIserver GeoProbe Adapters. This field is required when the ISA and Maps applications are deployed with SpIprobes. • Iris Maps uses the first IP address. • ISA requests are routed to the defined IP addresses by round robin. For example, if two IP addresses are defined, the first request is routed to the first IP address, the second request is routed to the second IP address, and the third request is routed to the first IP address. Refer to Iris Network Data Flow for information about how the GeoProbe ISA Adapter component works within the Iris network. Refer to Iris System Requirements for version requirements.
Geo/SpIserver Host Field	Enter a single valid IPv4 or IPv6 address corresponding to the GeoProbe SpIserver. This field is required to support applications deployed with SpIprobes.
Geo Cas Server Hostname Field	Enter the hostname corresponding to the GeoProbe SpIserver on which the Central Authentication Service (CAS) resides. This field is required to support applications deployed with SpIprobes. The default value of N/A indicates a G10-only deployment.
NGGEO Jboss Server Hostname Field	Enter the hostname corresponding to the GeoProbe SpIserver on which Jboss resides. This field is required to support applications deployed with SpIprobes. The default value of N/A indicates a G10-only deployment.

PTP Servers Area

PTP Server Field	Enter a single valid IPv4 or IPv6 address to define a PTP server the TD140 will use to synchronize time. The address listed here is listed in the TD140 Details tab. A TD140 can only be assigned one PTP server.

Servers Tab



Config Import Tab

The Import tab enables administrators to import data from one or more CSV-formatted files for *nodes* and *applications*; refer to Using CSV Import/Export for details. The Import feature also supports importing trunk mapping files; refer to Enabling ISUP H248/MGCP Correlation for ISA for details.

CSV File List Pane

The CSV File List pane shows the CSV files available for import from the current directory. You can import application, node, and trunk mapping files.

Import Source Path Field	You can change the source path used for importing one or more CSV files. The default source directory is the same as the default destination directory /export0/home/iris. Click the Change Directory button to navigate to a different path.
Change Directory Button	

File Check Boxes	Select specific CSV files to import by selecting their corresponding row check boxes. • Applications and Nodes - You can only select multiple files of the same type for import, not different types. For example, you can import multiple Application CSV files, but you cannot import an Application CSV file and a Node CSV file at the same time. • Trunk Mapping - Only one Trunk Mapping CSV file can be imported.
File Column	Lists all CSV files that reside in the specified location.
Type Column	Displays the type of CSV file - Applications, Nodes, or Trunk Mapping. Iris identifies the file type of each CSV file from its contents.
Import Button	Import data from the selected CSV files. Refer to the following sections for details. • Applications and Nodes • Trunk Mapping

Latest Import Summary Pane

The Latest Import Summary pane provides statistics for the most recent data import. Values appear one the import is complete.

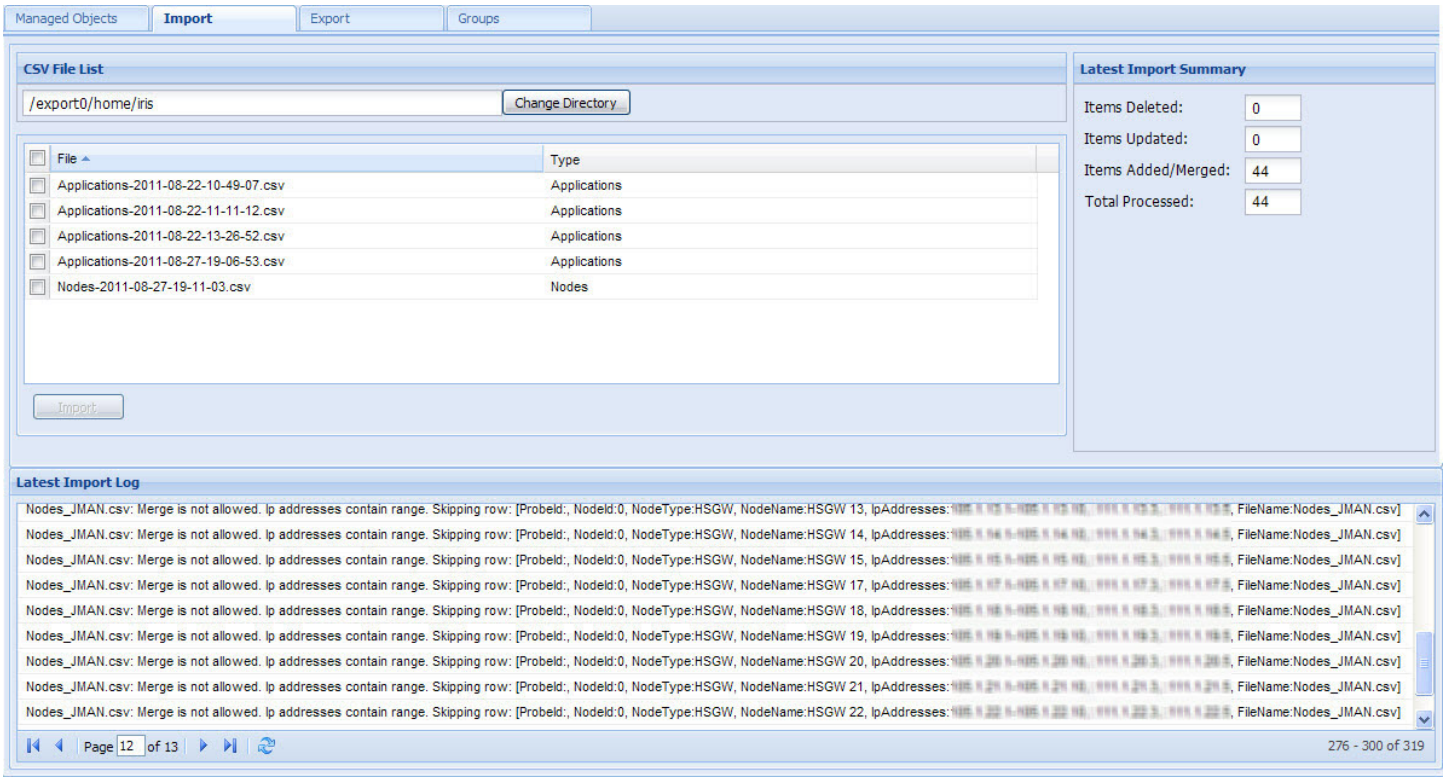
Items Deleted	Number of entities that were permanently deleted from the Iris system during the import process. This field does not apply to trunk mapping.
Items Updated	Number of entities for which information was modified. This field does not apply to trunk mapping.
Items Added/Merged	Number of entities that were added. For nodes, this value also includes counts for nodes merged into existing nodes. Refer to Automatic Node Merging for New Node Import for details. This field does not apply to trunk mapping.
Total Processed	• Applications and Nodes - Total number of entities deleted, modified, and added or merged. • Trunk Mapping - Total number of trunk mapping records processed.

Latest Import Log Pane

The Latest Import Log pane provides paged access to log messages for the most recent topology import. Log messages can include the following information:

- CSV filename
- Error messages
- Probe ID
- Node ID
- Application ID
- Node Name
- Application Name
- IP addresses
- Processing status (% complete)

Import Tab

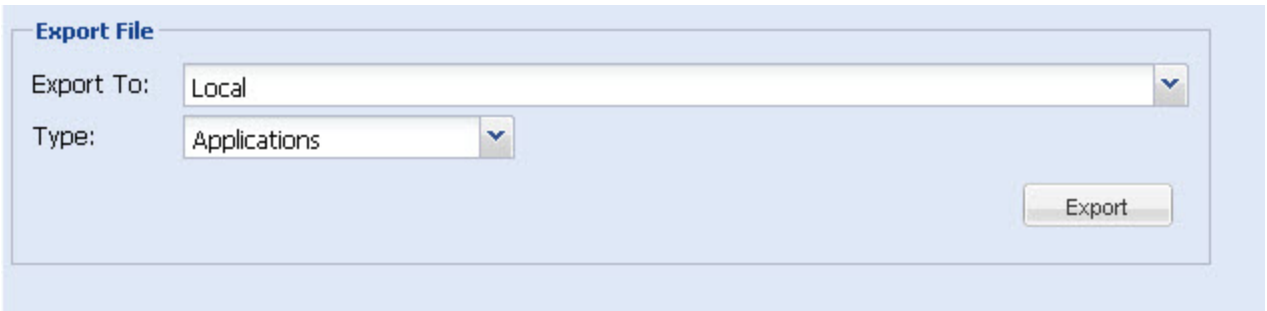


Config Export Tab

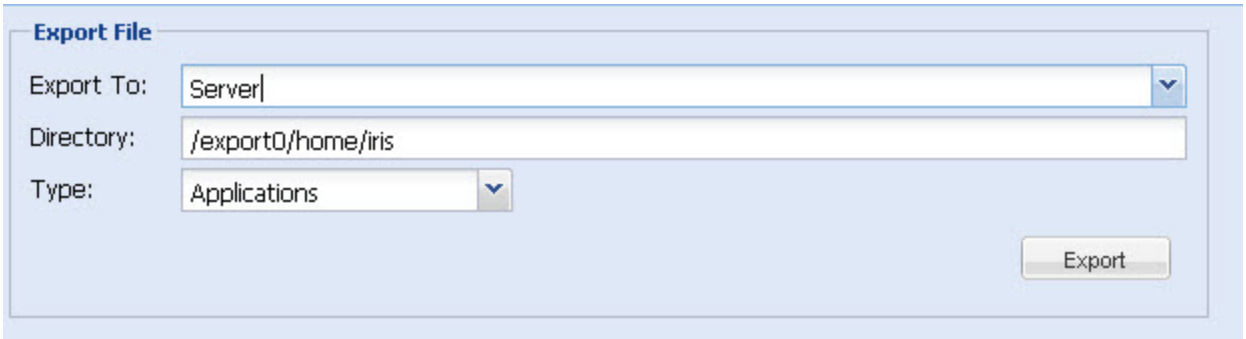
The Export tab enables administrators to export files into a CSV-formatted file; refer to CSV Import/Export for details. This tab does not apply to trunk mapping data; refer to Enabling ISUP H248/MGCP Correlation for ISA for details.

Export To Drop-down Menu Directory	• **Server** - save file to Iris server. The default destination path is /export0/home/iris, but you can modify it. • **Local** - save the file to your local drive. When you click Export, a Save File dialog box opens for you to select the folder.
Type Drop-down Menu	Select the CSV type for which you want to export data.
Export Button	Export all entity data to a CSV file. CSV files use the [EntityType]-yyyy-MM-dd-HH-mm-ss.csv naming convention. Refer to CSV File Formats for details.

Export Tab (Local)



Export Tab (Server)



Topology User Interface

Admin contains the following Topology GUI elements.

- Topology Tab
- Managed Objects Tab
- Entities Pane
- Application Details Pane
- Physical Link Details Pane
- Logical Link Details Pane
- Protocol Details Pane
- Node Details Pane
- Physical Links for Node Dialog Box
- Audit Log Dialog Box
- Groups Tab
- Auto Detection Tab
- Add Group Members Dialog Box

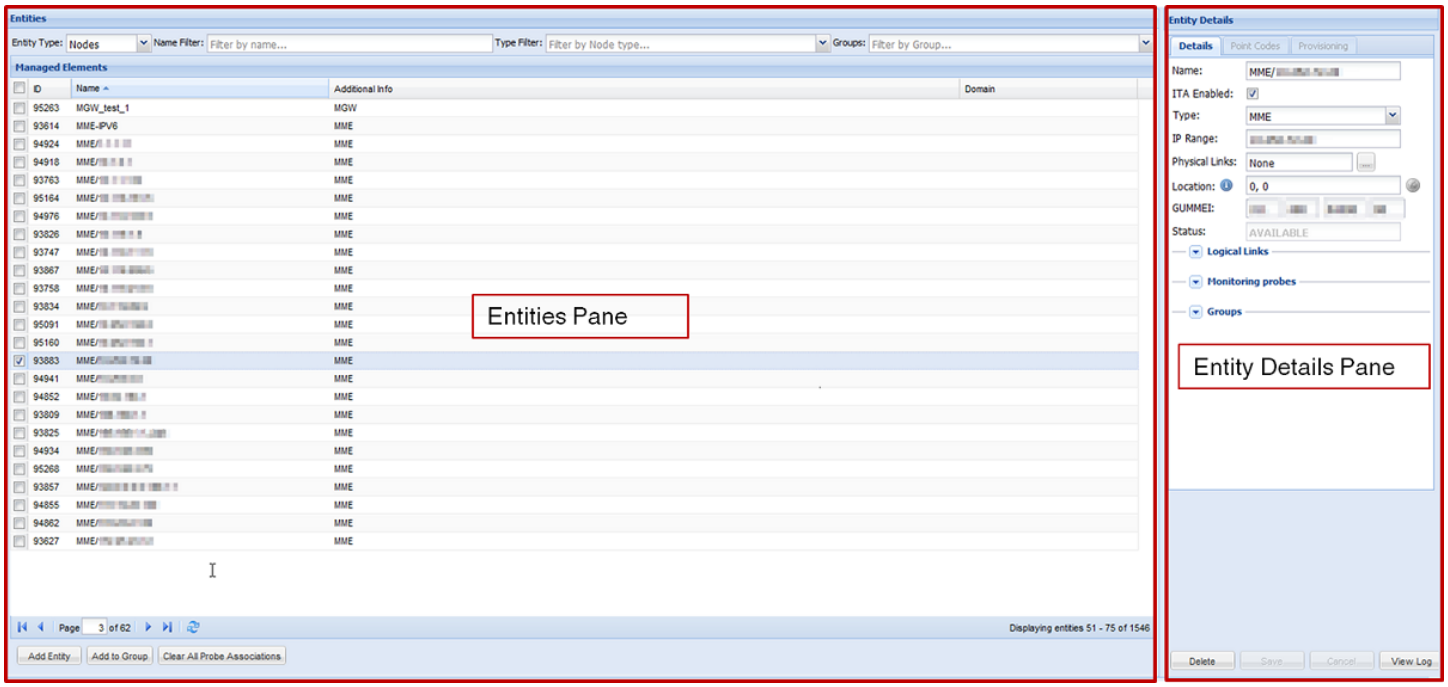
Topology Tab

The Topology tab enables you to define characteristics for each entity and add entities to specific groups to enhance logical monitoring capabilities for network operators in various geographic locations.

Topology Tabs

Managed Objects Tab	Manage Application Details, Physical Link Details, Logical Link Details, Protocol Details, and Node Details.
Groups Tab	Define entity groups for physical links, probes, and nodes. See Iris Application Support of Configured Entities for details on which Iris applications support entity groups.
Auto Detection Tab	Enable/disable per-probe topology auto-detection for all configured probes.

Topology Tab

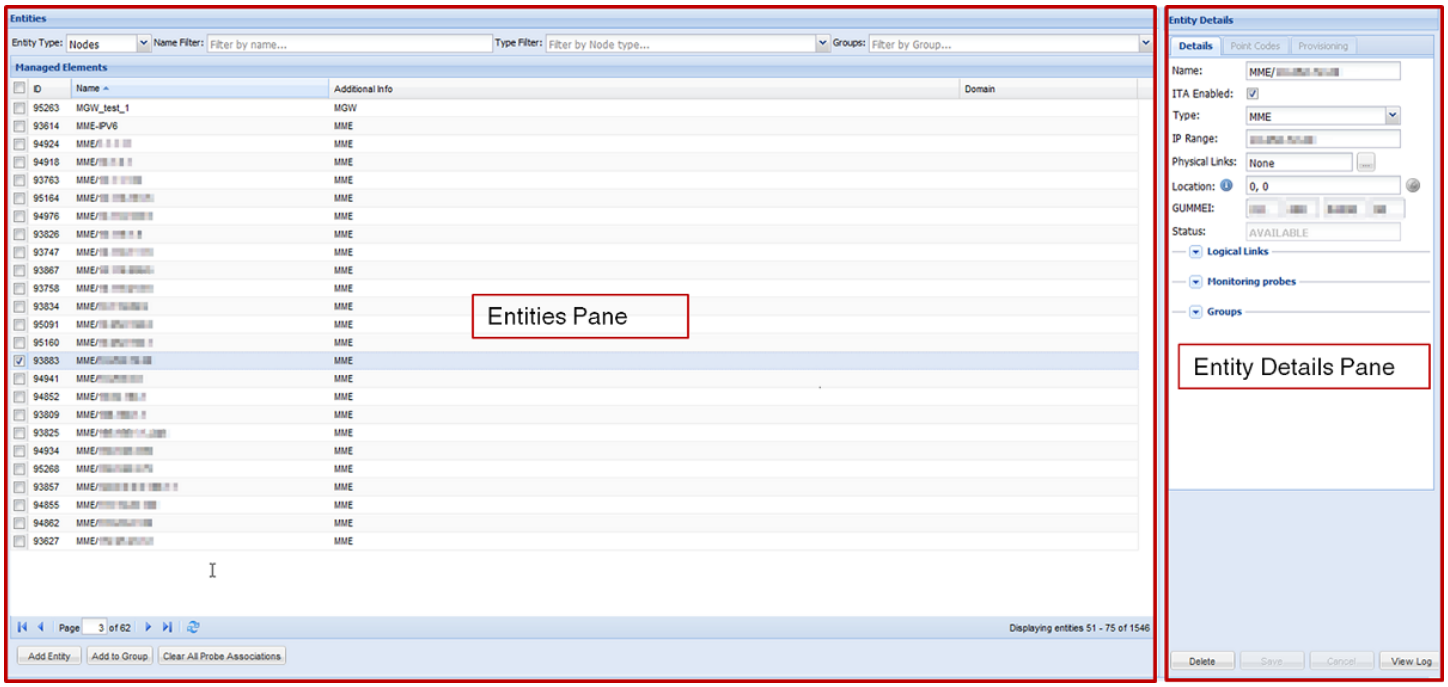


Managed Objects Tab

The Managed Objects tab is the main Topology view and enables you to view and configure nodes, protocols, applications, logical links, and physical links. You manage probes on the Probes Tab. The content on this window varies depending on which entity you filter.

Entities Pane	View a list of all currently defined entities and configure new entities.
Entity Details Pane	View and configure various details for a selected entity such as IP address and port. This pane varies depending on the entity type you select: • Application Details (purchasable option) • Domain Details • Physical Link Details • Logical Link Details • Protocol Details • Node Details

Managed Objects Tab



Entities Pane

On the Managed Objects tab, you can view and filter configured entities on this pane, add new entities, and add entities to configured groups.

Columns

ID Column	An internal identifier used by the Iris server.
Name Column	The name of the entity; you can edit the name in the Entity Details pane.
Additional Info Column	Varies per entity. Displays additional information about the entity such as the type of node.

Filter Controls

Entity Type Drop-Down Menu	Select an entity to use as a filter for the Managed Elements table.
Name Filter Field	Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Type Filter Drop-Down Menu	Applies to Nodes only. Select a node type to use as a filter for the Managed Elements table.
Groups Drop-Down Menu	Select a group name to use as a filter for the Managed Elements table. The drop-down menu lists all entity groups defined on the Groups Tab. Group names display in the format [Group Entity] - [Group Name].
Show Disabled Check Box	Applies to applications and protocols only. You cannot delete these entities, only disable them. Select this check box to display, in the Managed Elements list, those elements that were disabled in the Entity Details Pane.

Column Filters

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the check mark from columns you want to hide. At least one column must remain visible.

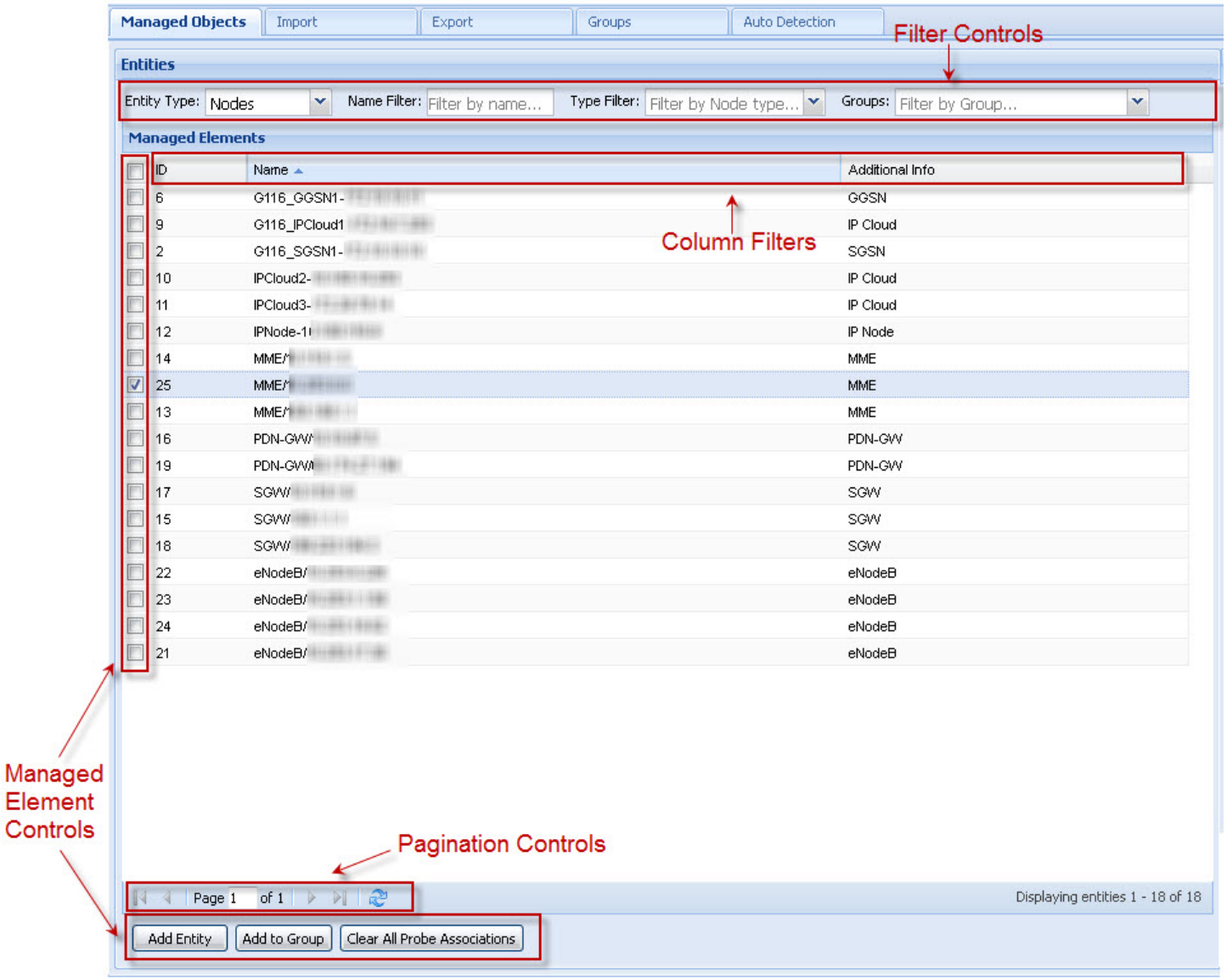
Managed Element Controls

Managed Elements Check Boxes	Select the top check box in the far left column to choose all entities in the list to add to an existing group. Or, select specific entities to add to a group by clicking on their corresponding row check boxes.
Add Entity Button	Open a blank Entity Details Pane for the entity type you are currently viewing.
Add to Group Button	Open the Add to Group dialog box and select one from a list of existing entity groups. Groups in which the entity is already a member are not listed for selection. Group names display in the format [Group Entity] - [Group Name]. Only physical link groups, node groups, and probe groups are supported in the current release. Refer Configuring Entity Groups for details.
Clear All Probe Associations	Only applies to nodes; removes all probe associations from all nodes.

Pagination Controls

Page Field	Enter a page number in the field and click the Next or Previous buttons to display the corresponding page content in the list pane. This enables you to quickly locate a specific page when there is a large number of items.
Next Button	
Previous Button	
Begin/End Buttons	Display the first page or the last page in the list.
Refresh Button	Manually refresh the list.

Entities Pane



Application Details Pane

You use the Application Details pane to configure traffic classification for applications (if you have purchased this license). You use the Protocol Details pane to configure traffic classification for protocols.

This pane varies depending on whether the application is a Tektronix-defined application or a custom application created by you. Refer to the ***Traffic Classification Configuration*** tutorial in the Admin online help for workflow details.

You can also manage applications using the Import/Export feature; refer to Using CSV Import/Export.

ID Field	An internal identifier used by the Iris server. IDs greater than 63000 indicate custom user-defined applications; IDs less than 63000 indicate Tektronix-defined applications.
Name Field	Add or change application name. Name must be unique to applications and protocols.
Description Field	Add or modify description.
Enabled Check Box	Select this check box to enable or disable the application. By default, all applications are enabled for monitoring by the Iris system.

UA/URL Parameters Area

This area is only accessible for user-defined applications; you cannot view or modify UA/URL parameters for Tektronix-defined applications. Classifying applications by User Agents and URLs enables you to view which applications running over HTTP are used in your network.

UA	Define UA/URL parameters based on the following rules:
	• "http://" or "https://" not allowed
	• URL format: host/URL
	• If null, leave blank; do not use "".
	• Separate multiple UA/URLs with commas (no spaces)
	• Only alphanumeric characters, and '.', '?', '%', '/', '_', '-', ':','=' characters are supported in URL string
	• Asterisk (*) can replace multiple characters only in the middle of a string; leading and trailing wildcards are assumed and are not allowed to be defined explicitly.
	  • Valid: yahoo.*/page
	  • Not valid: yahoo*
	See First Longest Match Criteria for details about how the probes analyze and match URLs.

URL	

IP Parameters Area

This area is accessible for both user-defined and Tektronix-defined applications. Classifying applications by IP/Port combination enables you to view hosted services or internal servers as applications, regardless of protocols that the services use.

Protocol Drop-Down Menu	The following components are used together to define IP parameter combinations:
	• Click **Add** to insert a blank row in the IP Parameters area.
	• Select a transport level (L4) protocol: TCP, UDP, or SCTP. For Application configuration, select the asterisk (*) to monitor all protocols for the port.
	• Enter one or more ports separated by a comma, a dash, or both.
	  • Two protocols cannot share a port and two applications cannot share a port; however, a port and an application can share the same port.
	• Enter one or more IP addresses or IP range using IPv4 or IPv6 format. See Supported IP Address Formats and Syntax for details.
	  • For protocols, if no IP address or range is defined, Iris monitors all traffic on defined ports; applications require you to define an IP address or range.
	  • Two protocols cannot share a port and two applications cannot share a port; however, a protocol and an application can share the same port.
	• Click **Add** again to add another row in the IP Parameters area. Click Delete to delete a highlighted row in the IP Parameters area.
	Click **Save** to save the application.

Port Range Field	
IP Range Field	
Add Button	
Delete Button	

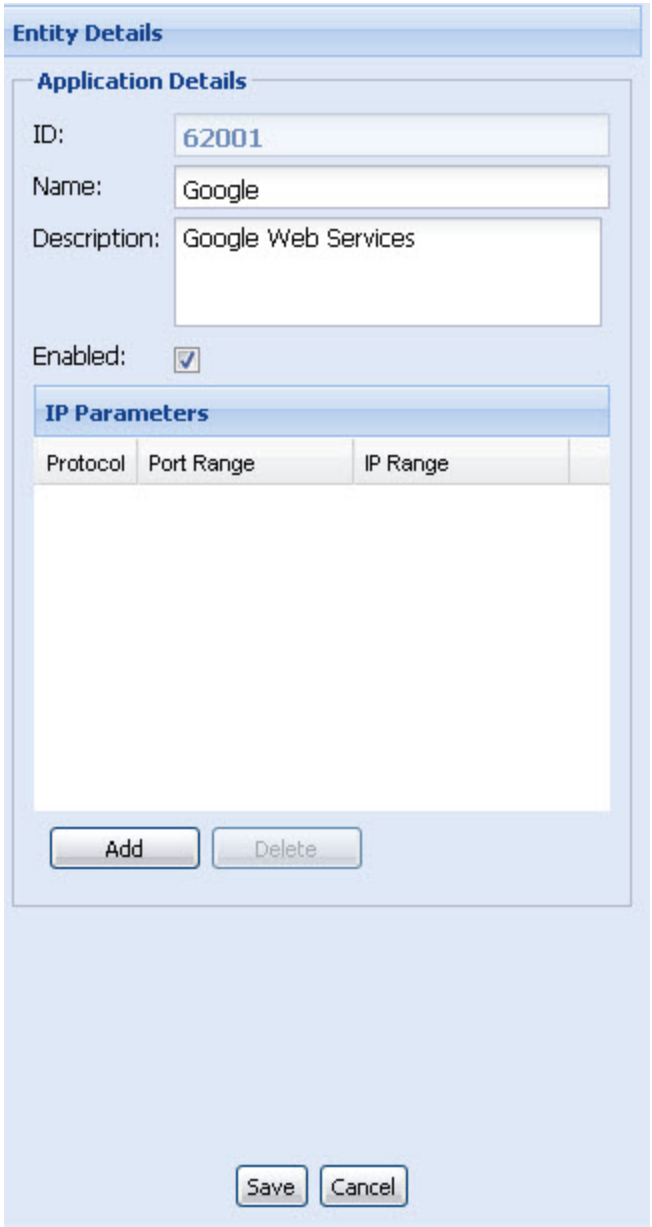
Entity Detail Controls

You can add a new entity and choose from the available options to define relevant entity details.

Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

Application Details Pane (User-Defined Application)

Application Details Pane (Tektronix-Defined Application)



First Longest Match Criteria

The G10 probes track UA/URLs using a "First Longest Match" criteria for matching UA/URLs. First Longest Match is a method where the G10 probe scans the UA/URLs seen in traffic and compares them to the defined UA/URLs until the first longest match is returned. The following table lists examples of the "First Longest Match" criteria.

URL Seen in Traffic	Defined URLs	Result
www.yahoo.com/sports	www.yahoo.com	www.yahoo.com
	www.yah.com	
	yahoo.*/page	
www.yahoo.com/sports	www.yahoo.com	www.yahoo.com has precedence over yahoo*/sports
	www.yah.com	
	yahoo.*/sports	
www.yahoo.com/maps/NorthAmerica/Canada/Quebec	yahoo*Canada	quebec will be chosen since full patterns have precedence over partial ones
	quebec	
	yahoo*mail	
finance.yahoo.com/stocks/ABC=231&DEF=300	DEF=300	Yahoo*stocks will be chosen since search terminates when "&" character is encountered
	yahoo*stocks	
http://www.tcpipguide.com/free/t_IPv6DatagramSize	Tcpip*free	Tcpip*free is chosen since it is the earliest match
	IPv6*Size	
www.yahoo.com/mail/inbox/John_doe	YAHoo.com	yahoo.com is chosen since it is the earliest match and patterns are case insensitive
	mail*doe	
	John_doe	

Supported IP Address Formats and Syntax

Formats	IPV4	IPV6
Simple	Single: 10.20.30.40 Multiple: 10.20.30.40, 11.22.33.44	Single: 0abe:feff:9898::6455 Multiple: 0abe:feff:NNNN::6455, 2001:db8:85a3:0:0:8a2e:370:NNNN
Range	Define a range of IP addresses with a dash (-); separate multiple IP ranges with commas (,). *Single Range* 10.20.30.40-10.20.30.50 *Multiple Ranges* 10.20.30.40-10.20.30.50,11.22.33.44-11.22.33.55	Not Supported
CSV File (Multiple IP Addresses)	Separate multiple IP addresses or multiple IP address ranges with a comma, and enclose in quotation marks. Multiple IP Address Example "10.20.30.40, 1.2.3.4" Multiple IP Ranges Example "10.20.30.40-10.20.30.50,11.22.33.44-11.22.33.55"	Separate multiple IP addresses with a comma, and enclose in quotation marks. Example "0abe:feff:NNNN::6455, 2001:db8:85a3:0:0:8a2e:370:NNNN"

Formats	IPV4	IPV6
Wildcard	Asterisk (*) 10.20.30.* 10.20.*.40	Not Supported
Classless Inter-Domain Routing (CIDR) Notation	CIDR notation specifies IP addresses and their associated routing prefix. CIDR notation appends to an IP address a slash character and the decimal number of leading non-zero bits of the routing prefix.	
	Forward slash (/) 10.20.30.40/24 Netmask 1-32	Forward slash (/) 0abe:feff:NNNN::6455/64 Netmask 1-64

Domain Details Pane

You can use the Domain Details pane to create and edit a domain and assign Anchor Nodes and Physical Links to a domain. You cannot change the Default domain name, but you can change any other domain names. You cannot delete the Default domain, and deleting any other domain with physical links will move those links to the Default domain.

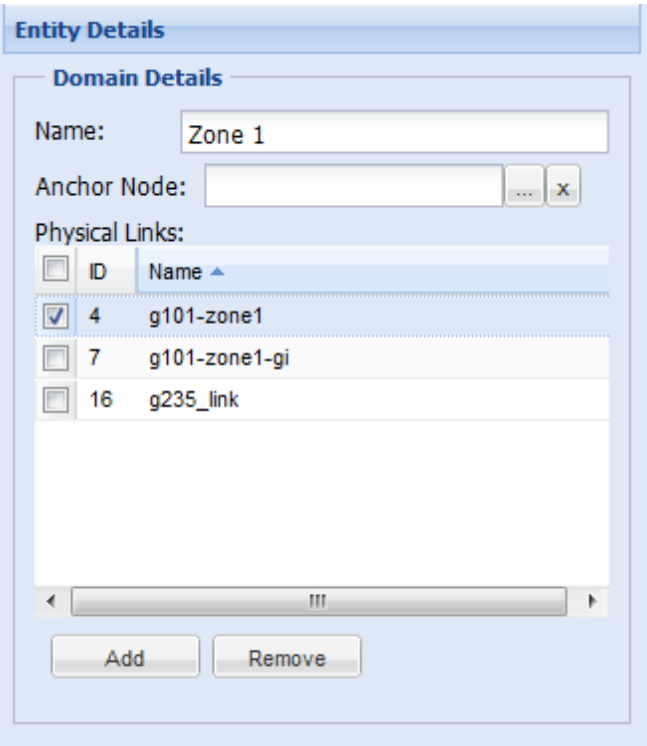
Name Field	Create a name for a new domain or edit the name of an existing domain.
Anchor Node Field	Click the ellipsis (**...**) next to the Anchor Node field to open the Anchor Node dialog box from which you can assign an anchor gateway node to the domain. The anchor gateway node must be either a PDN-GW or GGSN. Two domains cannot be anchored to the same anchor node. When an anchor node type is changed or removed, all of its anchored domains become unassigned.
Physical Links Check Boxes	Select one or more check boxes to enable the Remove button if you want to remove one or more physical links, or select the column header check box if you want to remove all of the physical links.
Physical Links ID Column	Internal IDs used by the Iris server.
Physical Links Name Column	Displays the names of the physical links.
Add Button	Open the Select physical links dialog box to select one or more physical links to add to the domain.
Remove Button	Select one or more physical links you want to remove and click this button.

Entity Detail Controls

You can add a new entity and choose from the available options to define relevant entity details.

Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

Domain Details Pane



Anchor Node Dialog Box

The Anchor Node dialog box enables you to select a physical anchor node to assign to a domain. You can access the Anchor Node dialog box by clicking the ellipsis (**...**) next to the Anchor Node field in the Domain Details pane. Only the PDN-GW and GGSN node types are available for selection as anchor nodes. Two domains cannot be anchored to the same anchor node. When an anchor node type is changed or removed, all of its anchored domains become unassigned.

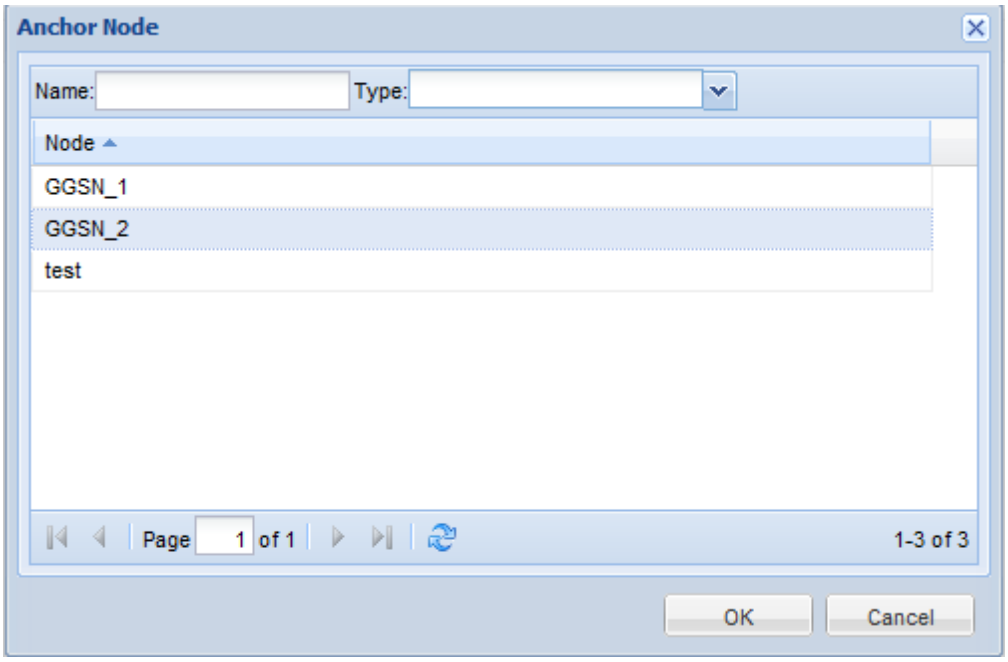
Columns

Node Column	View existing anchor node names and sort them alphabetically.

Window Controls

Name Filter Field	Filter anchor nodes by name. Enter one or more characters in the anchor node name and press Enter or Tab. • Filter is not case sensitive. • The system filters on all entity names containing the characters you type. • Matching elements appear in the file list.
Type Drop-down Menu	Select anchor nodes by type, GGSN or PDN-GW, or select All to show anchor nodes of both types.
OK Button	Apply the changes and close the dialog box.
Cancel Button	Close the dialog box without applying changes.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.

Anchor Node Dialog Box



Select Physical Links Dialog Box

The Select Physical Links dialog box enables you to select physical links you want to assign to a domain. You can access the Select Physical Links dialog box by clicking Add in the Domain Details pane. You cannot add the same physical links to a domain twice, and when you add a physical link to a domain it is removed from any other previously assigned domains.

Columns

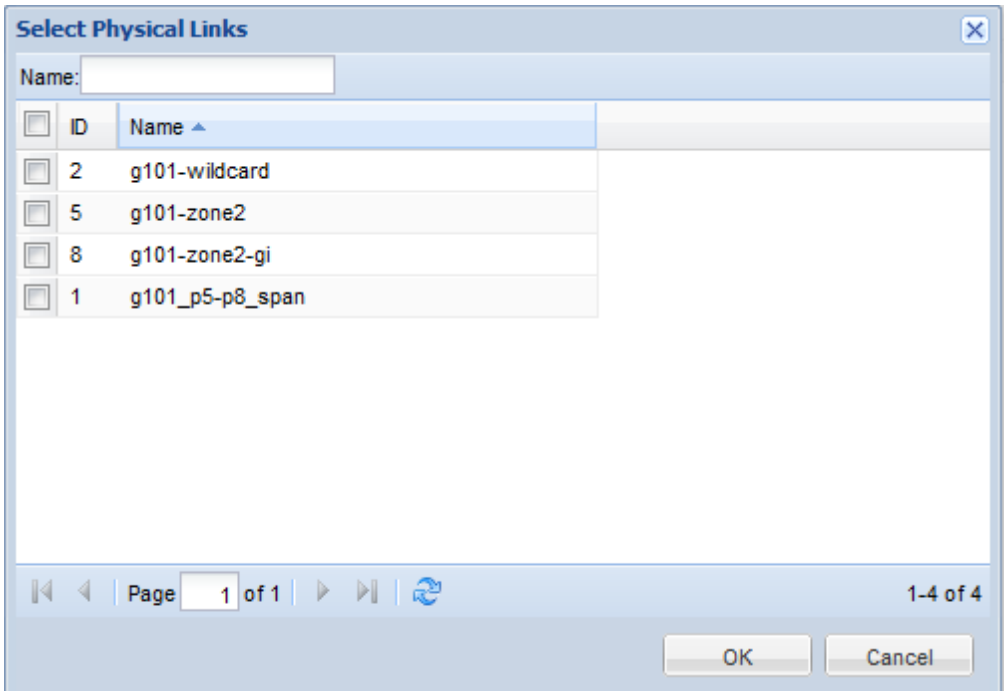
ID Column	An internal identifier used by the Iris server.
Name Column	The name of the physical link.

Window Controls

Name Filter Field	Filter physical links by name. Enter one or more characters in the physical link name and press Enter or Tab. • Filter is not case sensitive. • The system filters on all entity names containing the characters you type. • Matching elements appear in the file list.
Group Drop-down Menu	Filter probes by group name.
Show Used Only Check Boxes	Select this check box to filter the list of available physical links.
OK Button	Apply the changes and close the dialog box.

Cancel Button	Close the dialog box without applying changes.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.

Select Physical Links Dialog Box



Logical Link Details Pane

The Logical Link Details pane enables you to view configuration details for all logical links defined in the Iris system by manual configuration or auto-detection. This pane enables you to:

- Modify auto-detected logical links
- Add new logical links

Use this pane to customize individual logical links you want to monitor on your network; see Configuring Logical Links for details.

Name Field	Add or change the link name.
Server Node Field	Click the field or the button to select from a list of configured server nodes. If modifying an existing link, this field is read-only. *If a link has an incorrect endpoint defined, it must be deleted and recreated.*
Server Port Field	Enter the server port number to define the connection. Enter an asterisk (*) as a wildcard to monitor all ports for the link.
Client Node Field	Click the field or the button to select from a list of configured client nodes (eNodeBs in SCTP association). If modifying an existing link, this field is read-only. If a link has an incorrect endpoint defined, it must be deleted and recreated.

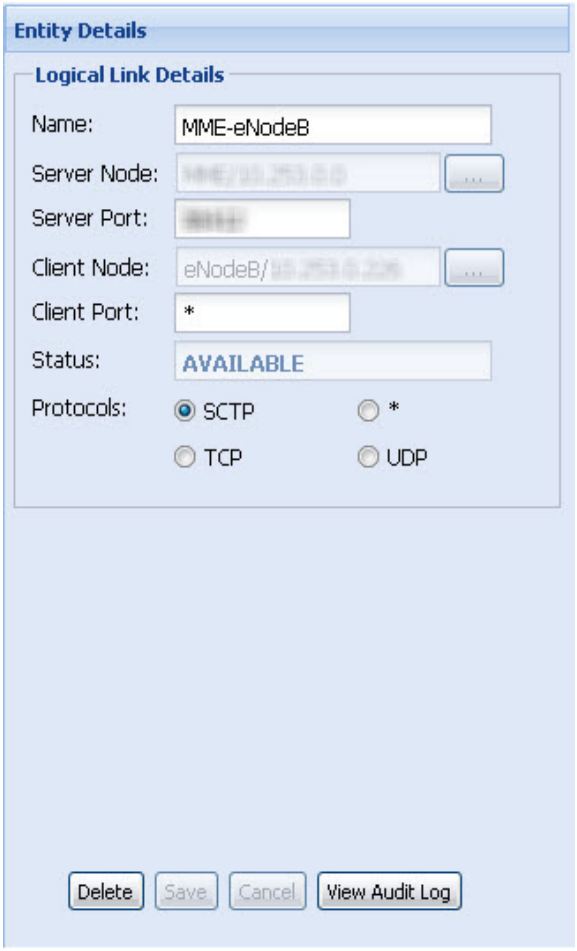
Client Port Field	Enter the client port number to define the connection. Enter an asterisk (*) as a wildcard to monitor all ports for the link.
Status	Indicates whether the logical link is available or in a maintenance state. When logical links are in a maintenance state, all LDV policy-based alarms associated with this link are not generated. A link's status is controlled by its associated nodes' maintenance status: • Logical links that have at least one associated node in a maintenance state have a maintenance state also. • As new logical links are added, if either of their endpoint nodes are in maintenance state, the link status is set to maintenance also.
Protocols Option	When manually configuring a logical link, select TCP or UDP as the transport protocol or select the asterisk (*) to indicate any transport protocol. Auto-detected SCTP associations have the SCTP option selected.

Entity Detail Controls

You can add a new entity and choose from the available options to define relevant entity details.

Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

Logical Link Details Pane



Node Details Pane

The Node Details pane enables you to view configuration details for all nodes defined in the Iris system by manual configuration, bulk import, or auto-detection. This pane enables you to:

- Modify auto-detected nodes
- Add new monitored network nodes
- Define specialized nodes such as:
  - Generic On-Demand nodes - Schedule node activation to target ITA statistics over a desired time frame.
  - Transparent Network Devices - These nodes can be created without IP addresses to represent devices such as routers, gateways, optimizers or firewalls. These nodes are typically assigned to physical links when monitoring IP networks. See the Physical Link Details pane for more information.

Use this pane to customize individual nodes you want to monitor on your network; see Configuring Nodes for details. You can also update multiple nodes at one time; refer to Using CSV File Import/Export for details.

Details Tab

Name Field	Add or modify the name of the node. Alphanumeric characters, minus (-), underscore (_), period (.), space, colon (:), or forward slash (/) are allowed. Auto-detected node names use the default "NodeType/IPAddress" or "NodeType/PointCode" syntax. Carrier- provisioned nodes names for MMEs and eNodeBs can be auto-detected from certain network maintenance message types; refer to Auto-detected Node Names for details.
ITA Enabled Check Box	Enable the node to collect transactional data for the ITA application. By default, all node types are enabled for the ITA application except for eNodeB, ePCF, and Generic-OnDemand node types. You can enable eNodeB and ePCF nodes as needed; however, you can only enable Generic-OnDemand Nodes through the scheduling feature.
Type Drop-Down Menu	Select or modify a node type for the node. The node type configured here overrides auto-detected and imported node types. For example, you can configure a node with the AAA node type and IP address 1.1.1.1. The G10 then detects IP address 1.1.1.1 on an S1-MME interface having an MME node type. The detected node type is ignored, and the node type for IP 1.1.1.1 remains as configured, node type AAA. ***If you want to change the node type of a node supporting point codes to a node type that does not support point codes, you must remove all defined point codes before you are able to change the node type.***
IP Range Field	Enter or modify the IP address or IP range using IPv4 or IPv6 format to associate with this node. The IP address must be unique and not match an existing node monitored by the same probe. See Active/Standby Node Provisioning for details. Iris applies node merging logic based on overlapping IP addresses, node type and other factors. IP addresses are optional for the Transparent Network Device node type and for select node types supporting point codes. When configuring nodes for tunneling protocols that will collect transactional data in ITA, it is recommended to configure the inner and outer IP addresses on separate nodes and to label them as such, for example: • InnerIP_Node • OuterIP_Node ITA does not display transaction detail information for outer IP addresses in tunneling protocols. ITA users will not see any data if they drill to Node or Node Group Transactions Detail pages from outer IP nodes on the Nodes or Node Group pages. Separating inner and outer IP addresses for nodes in tunneling protocols enables ITA users to more easily identify the tunneling protocol nodes from which they can drill for transaction details.
Physical Links	This field is only required if you are configuring redundant nodes; for example, when an IP address is shared between an active node and a standby node. See Active/Standby Node Provisioning for details. Click the **(...)** button to open the Physical Links for Node dialog box. ***This feature does not apply to SIGTRAN nodes.***

Location	Enter a Latitude and Longitude coordinate for the location you want the element to appear on Iris maps. Various Internet sites provide longitude and latitude coordinates when you enter address information. • Valid latitude coordinates are between -90 and 90 • Valid longitude coordinates are between -179.99 and 179.99 • Lat/Lon values separated by a comma or semi-colon can be copied from a source (such as the Internet) and pasted into either field; Iris automatically separates the values into separate fields • If no coordinates are defined, Iris will assign the default longitude and latitude values set in the Locations Tab. • You can also change a node's Lat/Lon values directly from the Iris Maps Overview window. Refer to the Iris Online Help for details. The Location icon indicates how the coordinates were set: • Gray - coordinates set by system based on mapping rules configured in the Locations Tab. The settings will automatically be updated with any changes to the Location rules or you can manually update the coordinates in this pane or directly on the map. • Green - coordinates were manually set; the settings will not be overwritten by updates to the Location rules.
GUMMEI fields	Enter or modify the GUMMEI digits for an MME node (optional). The GUMMEI must be unique and not match an existing MME. The maximum values for each field are: • MCC and MNC (first two fields) = 999 • MME GroupId (third field) = 65535 • MME code (fourth field) = 255
Status	Indicates whether the node is available or in a maintenance state. When a node is in a maintenance state, all LDV policy-based alarms associated with this node are not generated. A node's status is controlled by its associated probes' maintenance status. • Nodes that have at least one associated probe in a maintenance state have a maintenance state also. • As new nodes are added, if at least one of its associated probes are in a maintenance state, the node status is set to maintenance also.
Start Date	Define an activation schedule for Generic-OnDemand Nodes. This node type can only be active for a maximum of 6 hours for each activation period. Only 300 Generic-OnDemand nodes can be provisioned in the system at a time, and only 100 of these nodes can be activated at a time. Scheduling details are not exported for existing Generic-OnDemand node types. If an existing node is modified using the CSV Node Import feature and has a schedule associated with it, the schedule will remain the same. If a new OnDemand node type is added, its schedule will be empty, making it disabled at all times.
Start Time	
End Date	
End Time	
Logical Links	View a list of links for which the selected node is defined as an endpoint.
Monitoring Probes	View a list of probes that observed the current node in monitored traffic.
Groups	View a list of groups to which this node is a member. Defined groups appear as separate layers on maps. See Groups Tab for details.

Point Codes Tab

This tab is only available for select nodes types supporting point codes.

Point Code Field Network Indicator Drop-Down Menu Protocol Standard Drop-Down Menu Add Button Remove Button	The following components are used together to define point codes: • Click **Add** to insert a blank row. • Enter a point code in a valid format pattern for its corresponding Network Indicator and Protocol. Default point code formats are defined by Tektronix based on protocol (ANSI, ITU) and Network Indicator. You can customize point code formats based on your network requirements; contact Customer Support for details. • Select a Network Indicator and Protocol from the drop-down menus. • Click **Remove** to remove a highlighted row from the Point Codes tab. ***You must remove empty rows prior to saving the node.*** • ***If you want to change the node type of a node supporting point codes to a node type that does not support point codes, you must remove all defined point codes before you are able to change the node type.***

Provisioning Tab

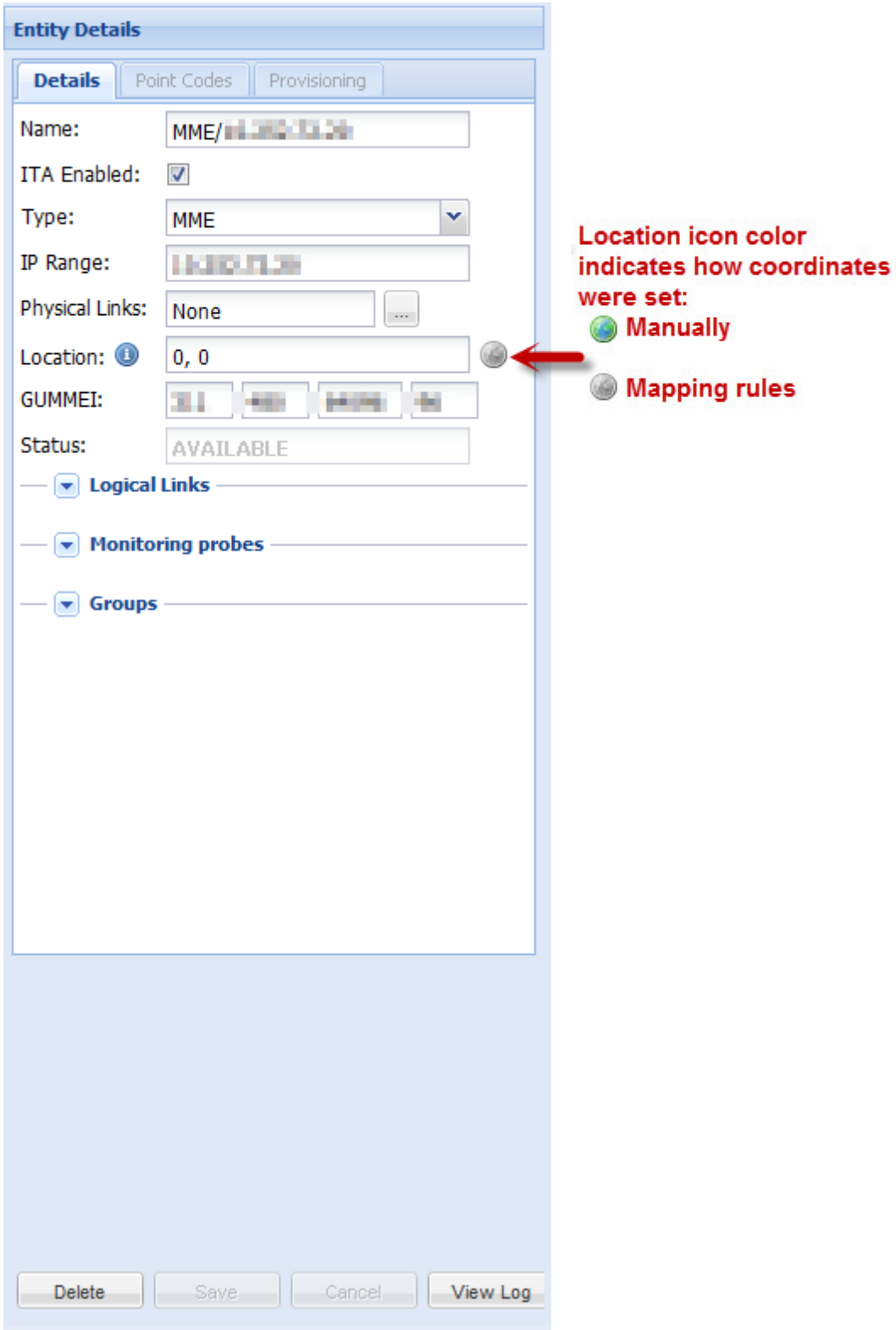
This tab is only available for per-probe nodes (currently Iris only designates auto-detected eNodeBs as per-probe nodes); it is grayed out for global nodes. It displays the ID and name of every probe that has been provisioned for this node.

Entity Detail Controls

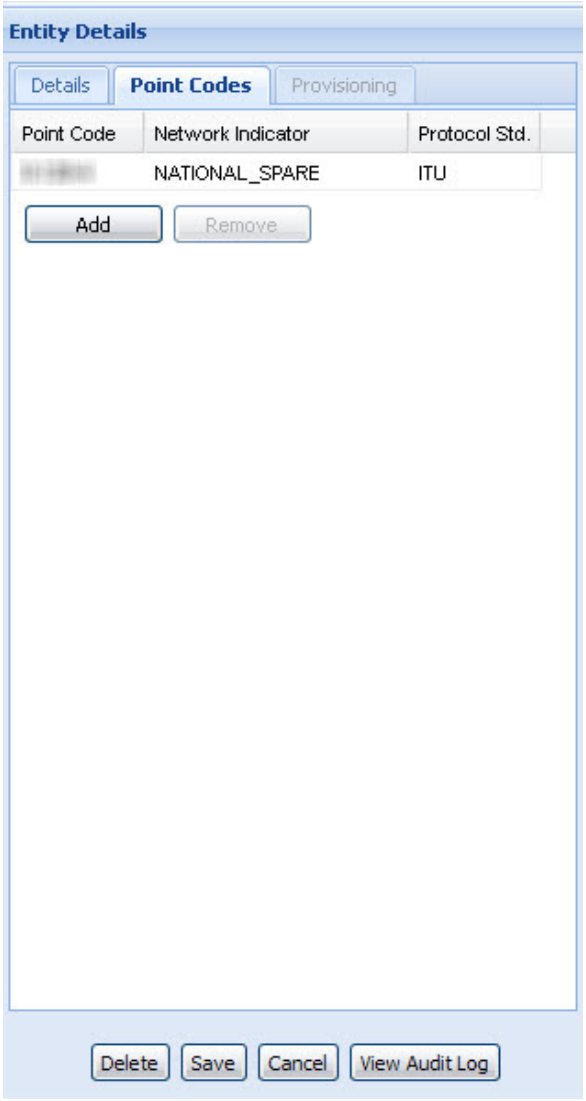
You can add a new entity and choose from the available options to define relevant entity details.

Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

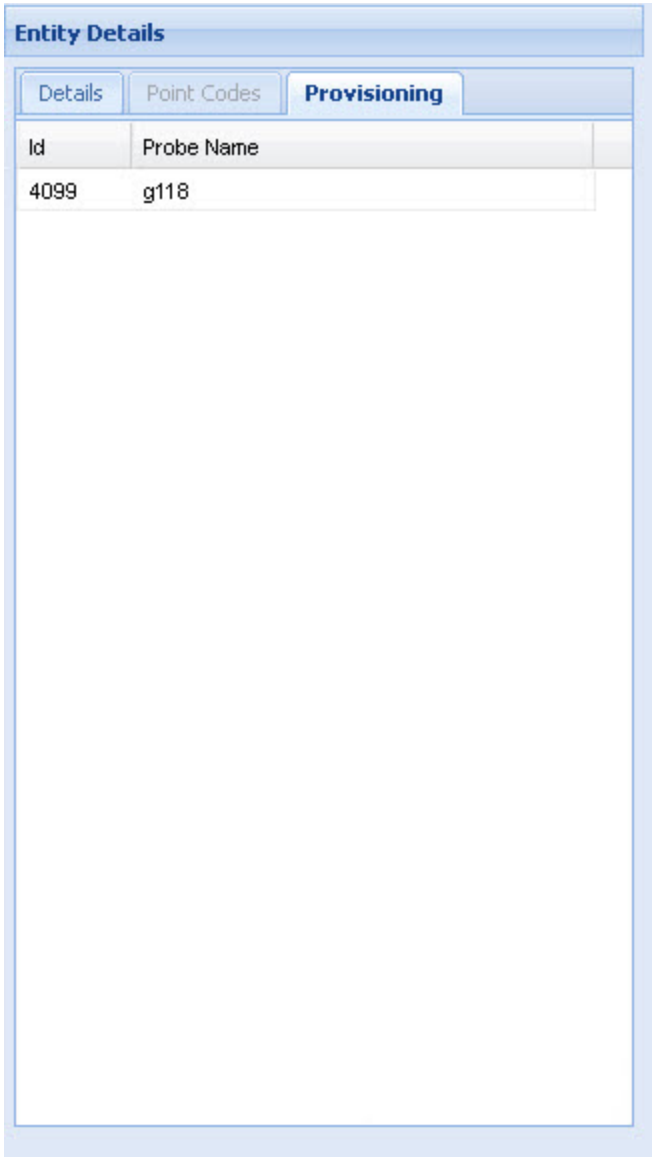
Node Details Pane - Details Tab



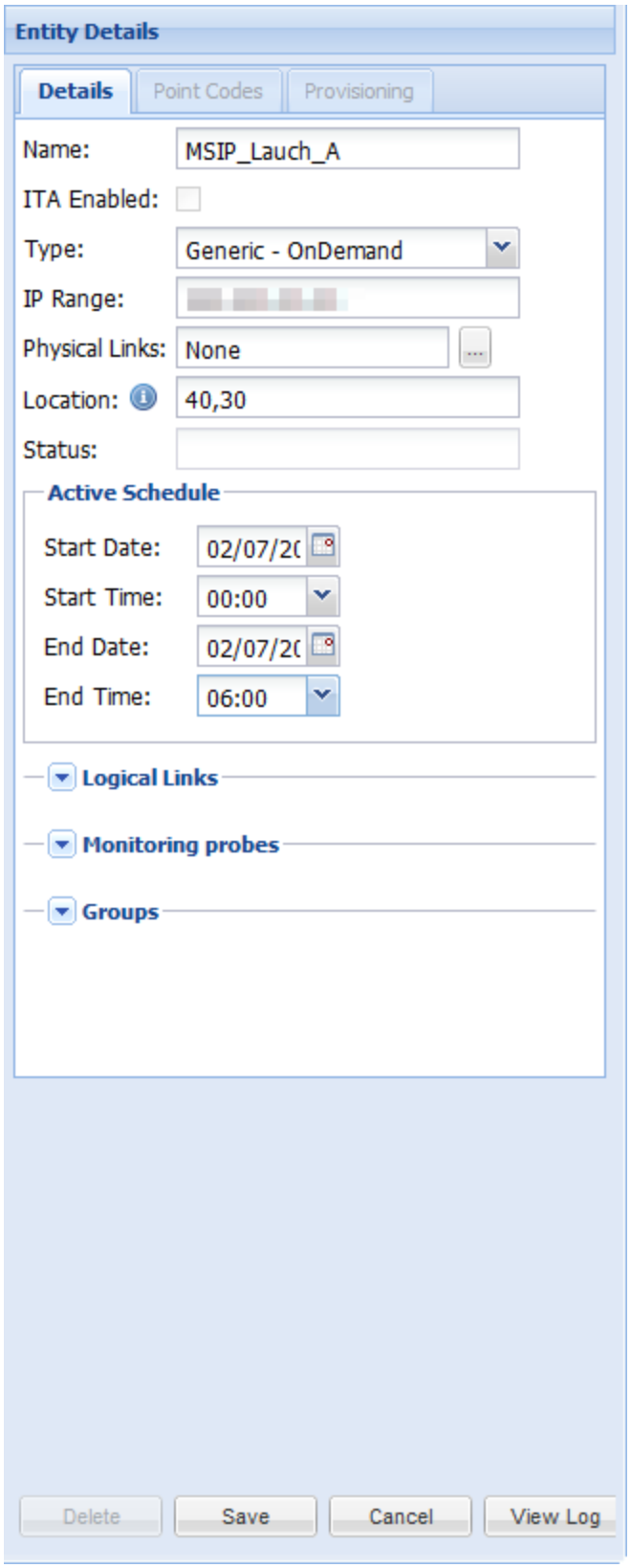
Node Details Pane - Point Codes Tab



Node Details Pane - Provisioning Tab



Node Details Pane - Generic-OnDemand Node



Physical Links for Node Dialog Box

You access the Physical Links for Node dialog box if you are configuring redundant nodes; for example, when an IP address is shared between an active node and a standby node. See Active/Standby Node Provisioning for details. You access it from the Node Details Pane.

This dialog box enables you to:

- Assign a probe to a node by selecting from the probe's physical links.
- View the assigned physical link ID.

This feature does not apply to SIGTRAN nodes.

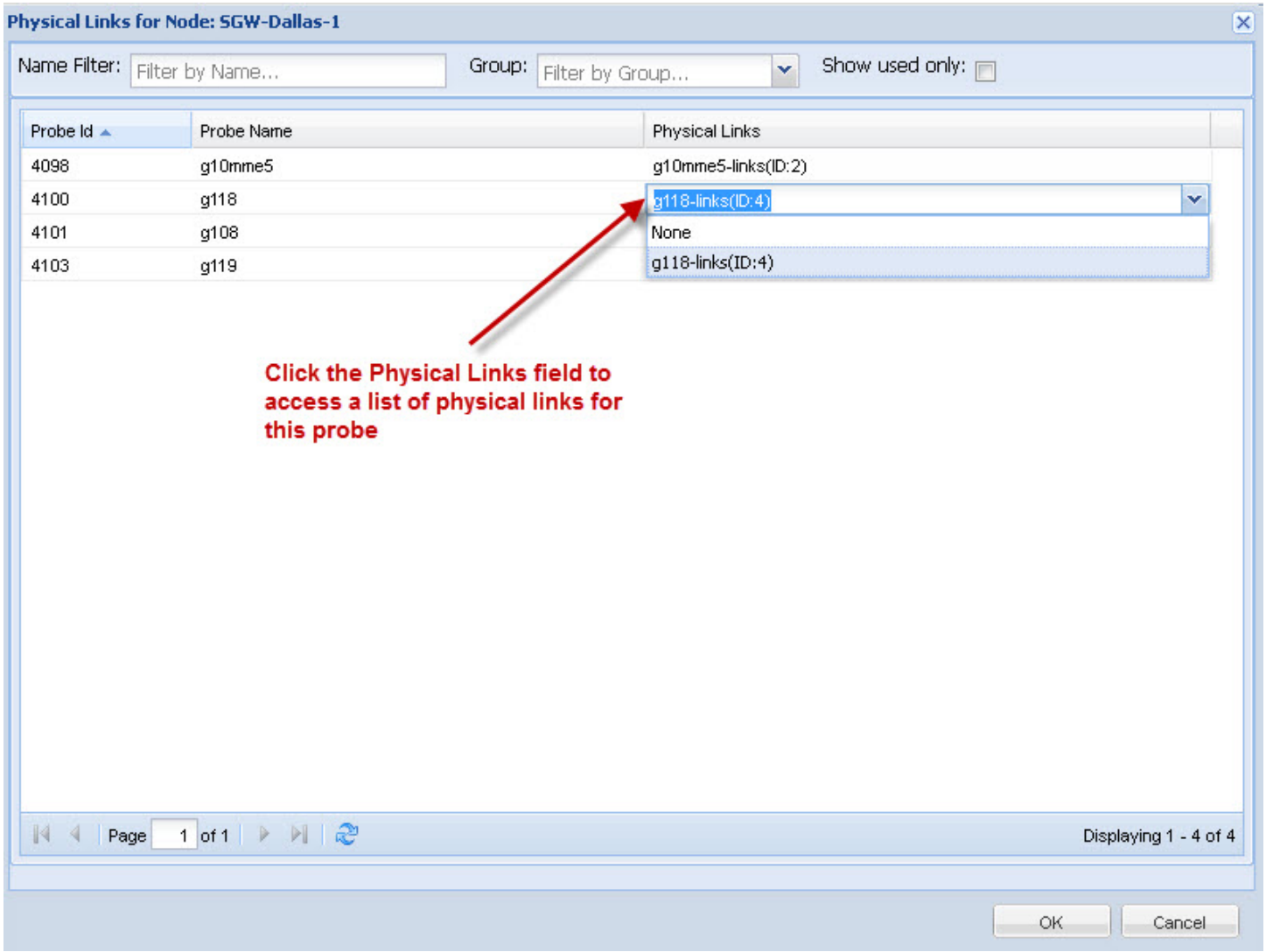
Columns

Probe ID Column	An internal identifier used by the Iris server.
Probe Name Column	The name configured for the probe.
Physical Links Column	Assign a probe to a node by selecting from the probe's physical links. You must assign at least one physical link to a node that is sharing an IP address with another node. • Physical links appear in LinkName (ID:PhysicalLinkID) syntax. Physical Links are configured on the Physical Links Details pane. • A node can have more than one physical link assigned to it only if the physical links are on different probes.

Window Controls

Name Filter Field	Filter probes by name. Enter one or more characters in the probe's name and press Enter or Tab. • Filter is not case sensitive. • The system filters on all entity names containing the characters you type. • Matching elements appear in the file list.
Group Drop-down Menu	Filter probes by group name.
Show Used Only Check Boxes	Select this check box to filter the probe list by probes that are already assigned to the current node.
OK Button	Apply the changes and close the dialog box.
Cancel Button	Close the dialog box without applying changes.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.

Physical Links for Node Dialog Box



Physical Link Details Pane

You use the Physical Link Details pane to map your G10 configured physical device ports or your TD140 ingress ports to links. These links can be used within Iris applications for filtering and viewing data per link or link group. For G10 IP monitoring, you can also configure node information for physical links to be used when viewing the ISA Ladder diagram (with "Show on Physical Link" view).

Link Details Tab

Map physical device ports to physical links and view the groups to which the link is a member.

Name Field	Add or change the link name.
Enabled Check Box	Enable or disable the link.

Probe Drop-Down Menu	Select the probe or TD140 to associate with the link. G10s bound to TD140s are not available for selection. When you select a TD140 device, the ingress ports appear in the Physical Device Ports area.
Enabled Check Box	Select to enable VLAN assignment: • If you select the Enabled check box, the Wildcard and Rx/Tx options become available. • Only values from 0 to 4095 (inclusive) are accepted for VLAN IDs. • Multiple physical links can share ports if they are mapped to different VLANs. • All enabled ports must be in Span mode when you assign VLANs. You cannot save your changes if any of the enabled ports are not in Span mode.
Wildcard	Select to find any VLANs associated with the selected physical device ports.
Rx/Tx	Select to assign VLANs to specific receiving and transmitting physical device ports. When you select this check box, Rx and TX fields appear. You must specify ports for both fields.
Physical Device Ports Check Boxes	Select the available physical ports you want to map to this link. These settings vary depending on deployment scenarios, including what kind of port was configured (tap or span). Contact Customer Support for assistance.
Groups	View a list of groups to which this physical link is a member.

Node Details Tab

This tab is applicable when monitoring IP networks and:

- G10 physical ports are configured as RX/TX taps (not span). Refer to Physical Device Port Configuration Examples for a graphical example of tapped ports connecting to a G10.
- IP flow records have been enabled for the physical link (configured by Tektronix). When IP flow records have been enabled for a physical link, every flow summary on the physical link generates an IP flow record which contains the flow summary. For example, POP3 packets result in an IP flow record containing a POP3 flow summary of the packets.

RX Node Field	These node settings are used to assign nodes to physical links to control data display in the ISA Ladder Diagram. Assigning nodes to physical links is typically used when each physical link represents a link in the network, and you want to use the configured nodes as endpoints for the packets on the link. This enables you to view the packet flow between the configured nodes in the ISA Ladder Diagram (with "Show Physical Link" option enabled). Refer to the Iris online help for more information about the ISA Ladder Diagram.

TX Node Field	**If Physical Link Endpoints are Known**
	• You can assign any node that is currently configured in the Iris system to a physical link; see the Node Details Pane and Configuring Nodes for details about configuring nodes for the Iris system.
	  ◦ Assign an **RX node** (destination node) to packets on the physical link or leave blank if destination node is unknown.
	  ◦ Assign a **TX node** (source node) to packets on the physical link or leave blank if source node is unknown

Select Node (...) button	**If Physical Link Endpoints are Unknown**
	• Enable the **Auto-generate nodes** option when **either** the RX node or the TX node or **both** nodes are unknown, or you do not want to configure nodes for the Iris system.
	  ◦ **Enabled (checked):** Iris auto-generates node name for an undefined RX or TX node. Destination node name format is "LinkName_DL"; Source node name format is "LinkName_UL"
	  ◦ **Disabled (unchecked):** IP addresses of packets will be used to determine any undefined RX or TX node.

Clear (x) button	• When **both** an RX and a TX node are defined for a link, the Auto-generate nodes option has no effect; each packet for the link will have the configured nodes as endpoints. • If no RX and TX nodes are defined, and the Auto-generate nodes option is disabled, Iris determines the endpoints based on the IP addresses of the packet.
Auto-generate nodes check box	Refer to the Node Details Configuration Matrix below to compare how different combinations of the Node Details settings affect the ISA Ladder Diagram behavior.

Node Details Configuration Matrix

The following matrix describes the behavior of the ISA ladder diagram when different combinations of the Node Details are configured.

Physical Link	RX Node	TX Node	Autogenerate	ISA Ladder Diagram Behavior
Link1	blank	blank	false	• IP addresses of packets will be used to determine endpoints. • Same behavior as having "Show Physical Link" option disabled in the ladder diagram.
Link1	blank	blank	true	• Each packet will have endpoints created based on the physical link name. • Endpoint names will use the following format: LinkName_UL / LinkName_DL. • Use this option if you do not want to configure nodes for Iris system.
Link1	Node1	Node2	false / true	• Each packet will have the endpoints Node1 and Node2. • Autogenerate has no effect.

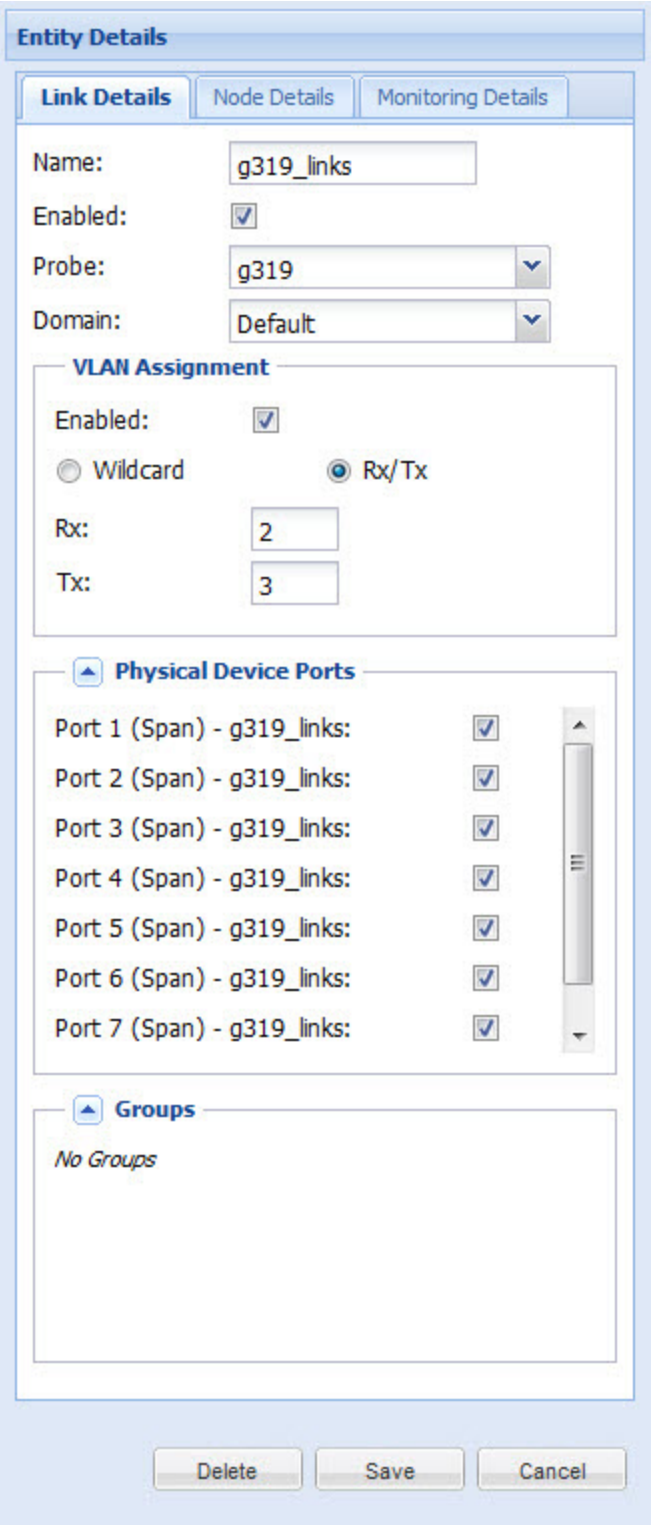
Physical Link	RX Node	TX Node	Autogenerate	ISA Ladder Diagram Behavior
Link1	Node1	blank	false	• Each packet will have Node1 as the destination node. • The source node will be determined based on the source IP address of the packet. • Useful for when destination node is known, but there are multiple source nodes.
Link1	blank	Node2	false	• Each packet will have Node2 as the source node. • The destination node will be determined based on the destination IP address of the packet. • Useful for when the source node is known, but there are multiple destination nodes.
Link1	Node1	blank	true	• Each packet will have Node1 as the destination node, and Link1_UL as the source node. • Useful for when you want to group all the source nodes of a link into one node, and you do not care about each individual node, such as monitoring a gateway / server.
Link1	blank	Node2	true	• Each packet will have Node2 as the source node, and Link1_DL as the destination node. • Useful for when you want to group all destination nodes of a link into one node, such as monitoring a roaming link.

Entity Detail Controls

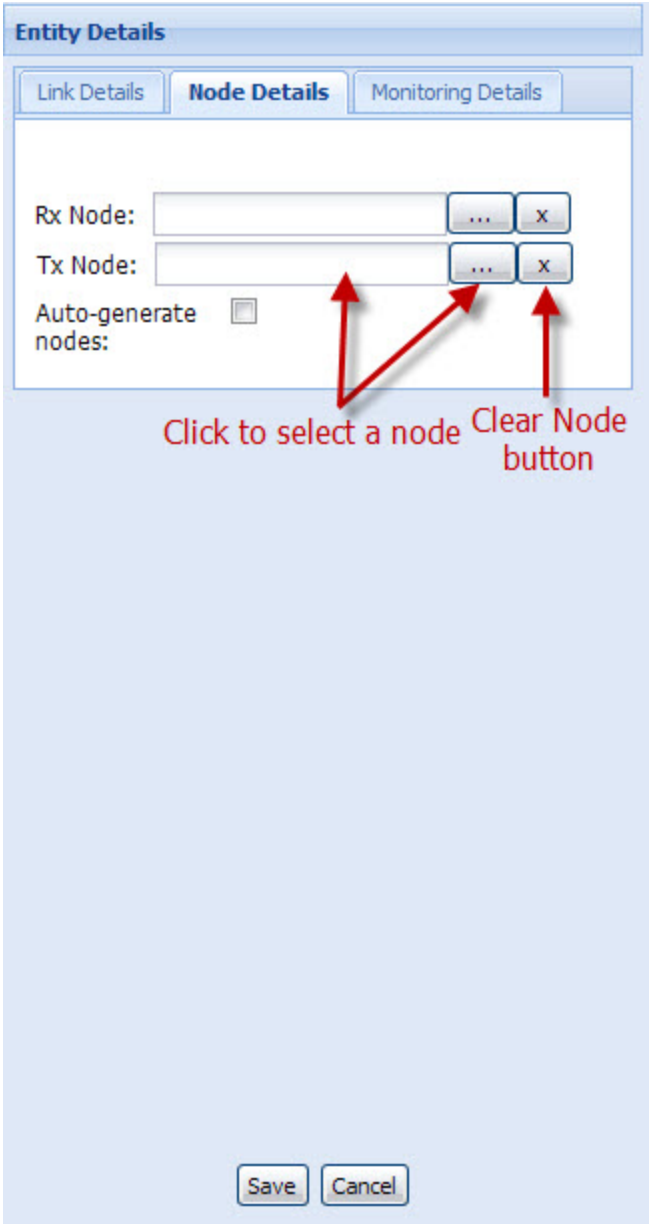
You can add a new entity and choose from the available options to define relevant entity details.

Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

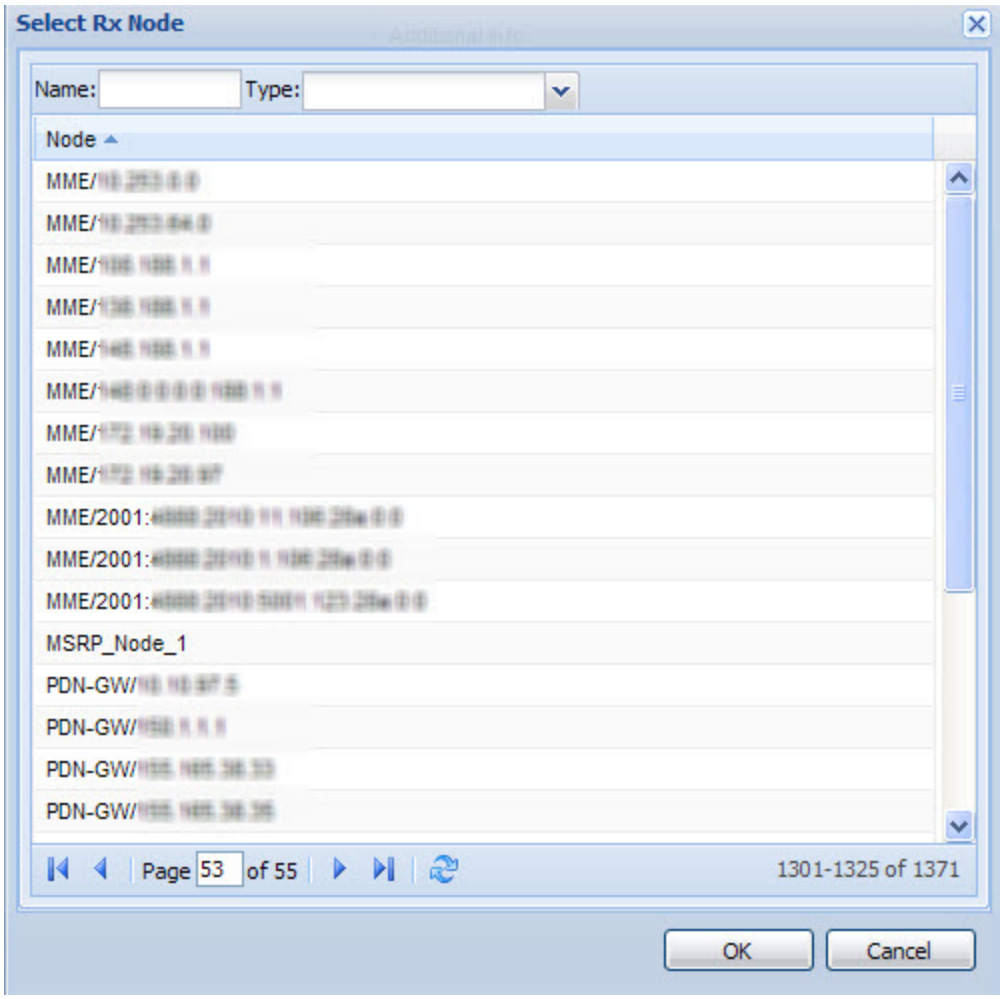
Physical Link - Link Details Tab



Physical Link - Node Details Tab



Select Node Dialog Box



Protocol Details Pane

You use the Protocol Details pane to configure traffic classification for protocols (such as for servers running services on non-standard ports). You use the Application Details pane to configure traffic classification for applications.

This enables Iris to correctly identify traffic for features such as ISA session trace, KPIs, and XDRs. Refer to the ***Traffic Classification Configuration*** tutorial in the Admin online help for workflow details.

ID Field	An internal identifier used by the Iris server.
Name Field	Add or change protocol name.
Description Field	Add or modify description.
Enabled Check Box	Select this check box to enable or disable the protocol. By default, all protocols are enabled for monitoring by the Iris system.

Entity Detail Controls

You can add a new entity and choose from the available options to define relevant entity details.

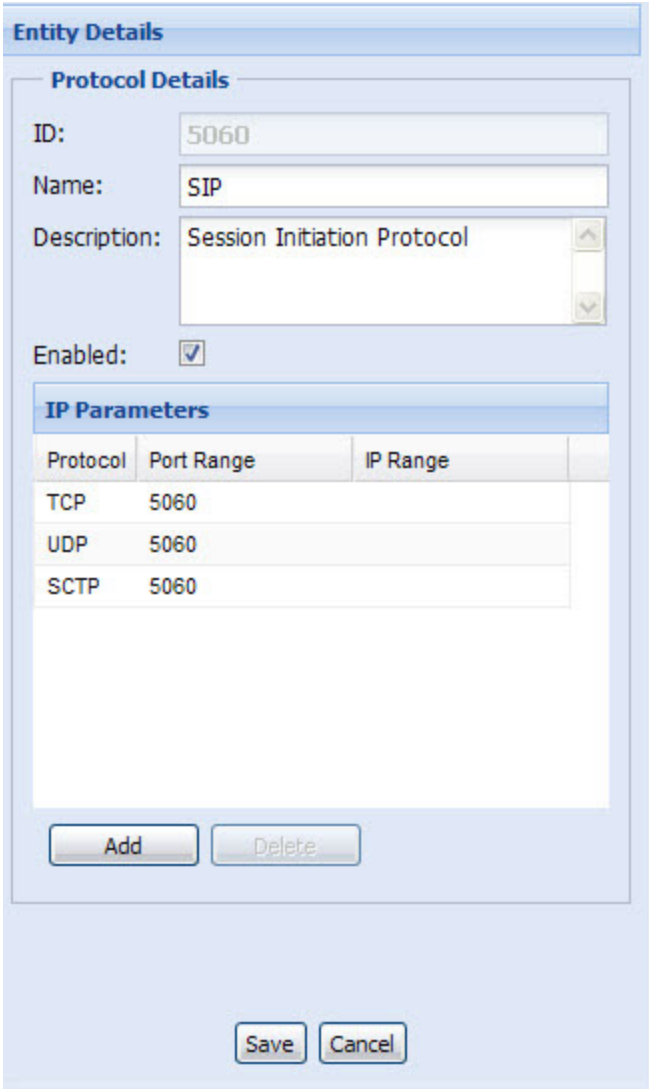
Delete Button	Delete the currently selected entity. You can only delete one entity at a time using this option. You cannot delete protocols; you can only disable them. • **Applications:** Permanently delete an application you defined. You cannot delete Tektronix default applications such as Google and HTTP-Video; you can only disable these applications. • **Links**: Permanently delete the current logical link. • **Physical Links:** Permanently delete the current physical link. You cannot delete a physical link which has nodes associated with it or a physical link which is a member of a group. • **Protocols:** You cannot delete protocols; only disable them. • **Nodes**: Permanently delete the current node and any associated logical links and probe associations. Deleted nodes having associated data appear in Iris applications labeled only with their IP address or point code. You can only delete one node at a time.
Save Button	Save the entity data to the master topology. Once a logical link is saved, the Server Node and the Client Node fields become read-only.
Cancel Button	Close the Entity Details pane without saving changes.
View Audit Log	Opens the Audit Log Dialog Box displaying the history of logged events for that specific element. This button is only available for logical links and nodes.

IP Parameters Area

Protocol Drop-Down Menu	The following components are used together to define IP parameter combinations:
	• Click **Add** to insert a blank row in the IP Parameters area.
	• Select a transport level (L4) protocol: TCP, UDP, or SCTP. For Application configuration, select the asterisk (*) to monitor all protocols for the port.
	• Enter one or more ports separated by a comma, a dash, or both.
	  • Two protocols cannot share a port and two applications cannot share a port; however, a port and an application can share the same port.
	• Enter one or more IP addresses or IP range using IPv4 or IPv6 format. See Supported IP Address Formats and Syntax for details.
	  • For protocols, if no IP address or range is defined, Iris monitors all traffic on defined ports; applications require you to define an IP address or range.
	  • Two protocols cannot share a port and two applications cannot share a port; however, a protocol and an application can share the same port.
	• Click **Add** again to add another row in the IP Parameters area. Click Delete to delete a highlighted row in the IP Parameters area.
	Click **Save** to save the application.

Port Range Field	
IP Range Field	
Add Button	
Delete Button	

Protocol Details Pane



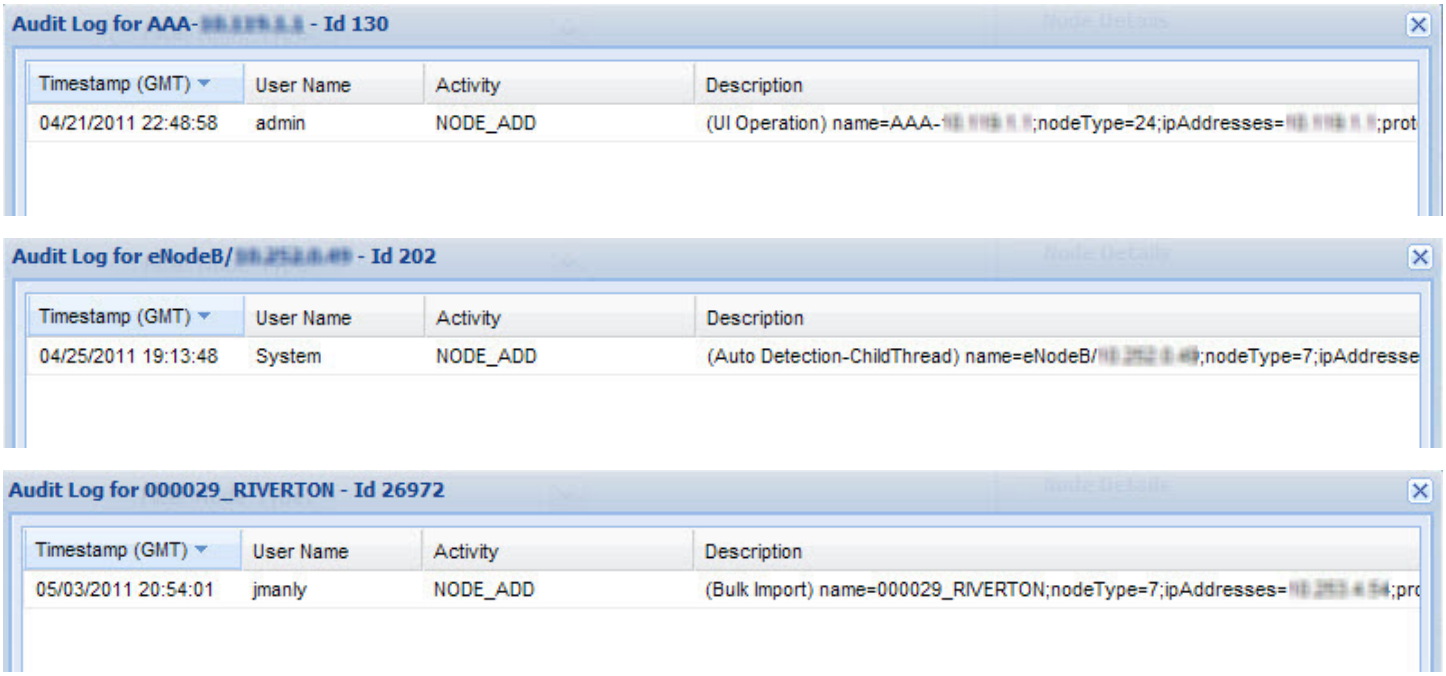
Audit Log Dialog Box

The Audit Log dialog box enables you to view the change history of the selected node or logical link. You access this window by clicking the View Audit Log button on the Node Details Pane or the Logical Link Details pane.

Timestamp	Iris client timezone.
User name	User ID of user performing action.

Activity	One of the following activities: • NODE_ADD • NODE_UPDATE • NODE_DELETE • LOGICAL_LINK_ADD • LOGICAL_LINK_UPDATE • LOGICAL_LINK_DELETE
Description	Provides the following information: • Operation: UI operation (from Topology tab), bulk import, or automatic topology detection • Logical Link Details or Node Details

Audit Log Dialog Box



Groups Tab

The Groups tab enables you to define entity groups to enhance group monitoring capabilities for Iris applications. Groups are only supported for physical links, probes, and nodes in the current release. Refer to Iris Entity Support for details on which Iris applications support entity groups. GeoProbe node groups can only be configured and maintained in GeoProbe. Refer to GeoProbe documentation for more details about GeoProbe system configuration.

Every group defined in the Iris system is a separate layer that can be viewed or hidden on Iris maps. You can define Iris entity groups to monitor certain elements together on the same layer in an Iris map. Iris Maps is installed with a default All Probes group which cannot be modified or deleted.

Groups Pane

The Groups pane enables you to edit existing groups and create new group types and groups. Groups are only supported for physical links, probes, and nodes in the current release.

Refer to Iris Entity Support for details on which Iris applications support entity groups.

Group Tree	Tree view containing Group Type folders. You can expand the folders to view groups contained in each group type.
New Type Button	Open the Group Type dialog and enter the name of a new group type.
New Group Button	Open the Group dialog, select the Group Type to which you want the group to be a member, and enter a name for the new group. • Group names must be unique across all groups, regardless of Group Type. • Allowable characters include alphanumeric characters, minus (-), underscore (_), period (.), space ( ), colon (:), or slash (/).
Edit Button	Select a Group Type or Group and click Edit. • Group Type - edit Group Type name • Group - change the assigned group type and edit the group name
Delete Button	Select a Group Type or Group and click Delete. • Group Type - delete selected group type and all associated groups • Group - delete selected group; all associated members are removed from the group

Members Pane

The Members Pane enables you to Add and remove members for each group and move members between groups. Groups are only supported for physical links, probes, and nodes in the current release.

Refer to Iris Iris Entity Support for details on which Iris applications support entity groups.

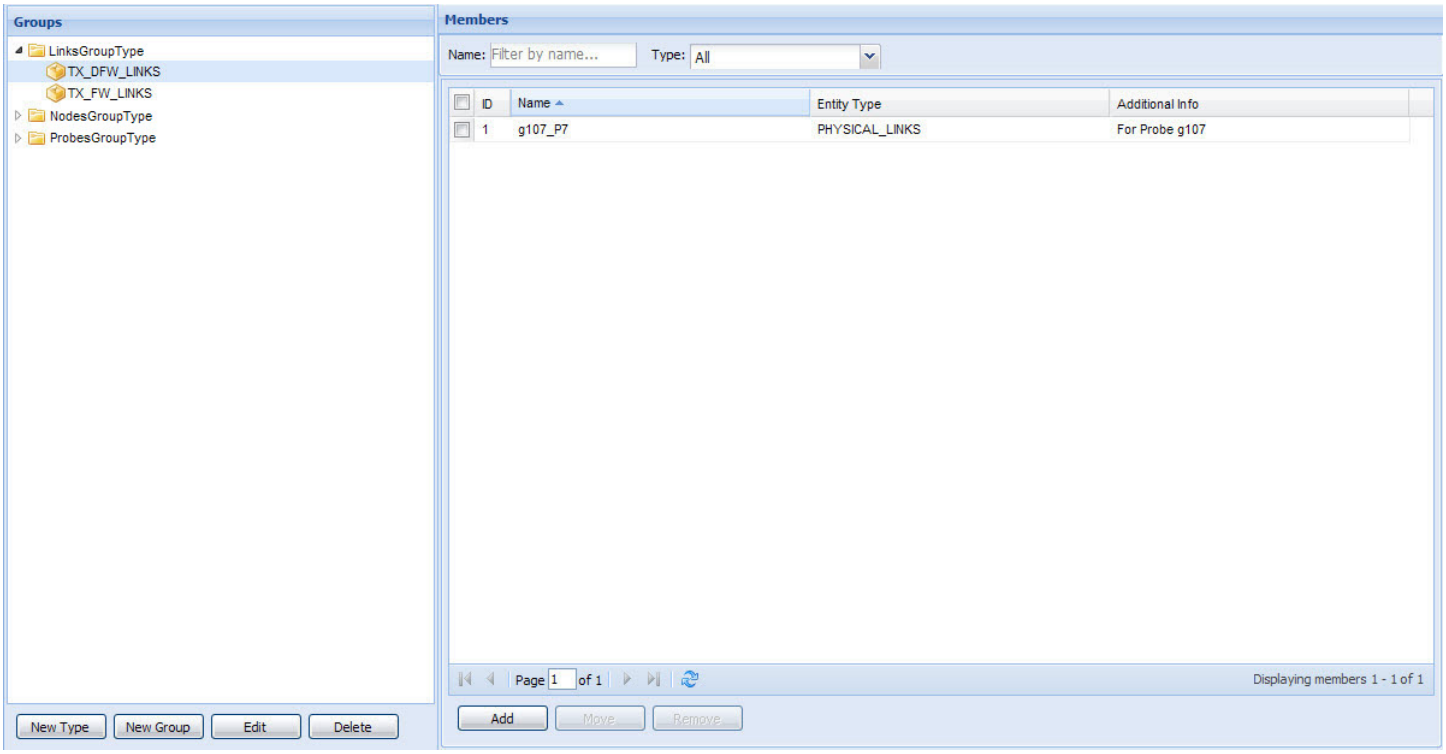
Name Filter Field	Search the group members by name. Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Type Filter Drop-down Menu	Select an entity type to use as a filter.
Members Check Boxes	Select the top check box in the far left column to choose all entities in the list. Or, select specific entities by clicking on their corresponding row check boxes.
ID Column	An internal identifier used by the Iris server.
Column Filters	You can apply a sort filter or show or hide columns using an actions menu.
Name Column	The name of the entity.
Entity Type Column	The type of entity.
Additional Info Column	Varies per entity; displays additional comments describing entity.

Page Buttons	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.
Add Button	Open the Add Group Member(s) Dialog Box dialog box to add members to existing groups.

Move Button	Open the Move Members To... dialog box to select a group to move the selected entities. Groups in which the entity is already a member are not listed for selection.
	• Group names display in the format [Group Entity] - [Group Name].
	• Groups will not be available for you to select if the entities:
	  • are already associated with the selected group.
	  • belong to another group within the same group type.

Remove Button	Remove selected members from the current group.

Groups Tab



Auto Detection Tab

The Auto Detection tab enables you modify topology commit enable/disable settings to all G10 probes.

The Enabled or Disabled status of these check boxes are copied to all G10 probes when you click the Apply to all Probes button. Note that these check boxes do not indicate the current topology commit state (enabled/disabled); you can view/modify a probe's current topology commit state on the Probe Monitoring Details tab.

Auto Node Topology Commit Enabled Check Box	Apply the following topology commit settings to all G10 probes. **Enabled** • Newly discovered nodes are committed by the Iris Server to the master topology and the Topology Tab is updated. • Per-probe nodes are associated with the probe that discovered them. You can view probe-to-node associations for per-probe nodes on the Provisioning tab on the Node Details Pane. • Iris server continues to update probe associations for **existing** per-probe nodes. • Auto-detected element updates are logged in the Audit Log. **Disabled** • Newly discovered nodes are NOT added in the system; the server will not add any new nodes (even per-probe nodes) discovered by the probes. • Iris server continues to update probe associations for **existing** per-probe nodes.
Auto Link Topology Commit Enabled Check Box	Apply the following topology commit settings to all G10 probes. **Enabled** • Newly discovered links are committed by the Iris Server to the master topology and the Topology Tab is updated. • Auto-detected link updates are logged in the Audit Log. **Disabled** • Newly discovered links are NOT added in the system; the server will not add any new links discovered by the probes.
Apply to all probes Button	When clicked, the settings on this window are copied to every probe's Monitoring Details tab, where you can adjust the settings for individual probes.

Auto Detection Tab

Add Group Members Dialog Box

The Add Group Members dialog box enables you to add entities to existing groups. You access it from the Members Pane on the Groups Tab.

Columns

ID Column	An internal identifier used by the Iris server.
Name Column	The name of the entity.
Additional Info Column	Varies per entity; displays additional comments describing entity.

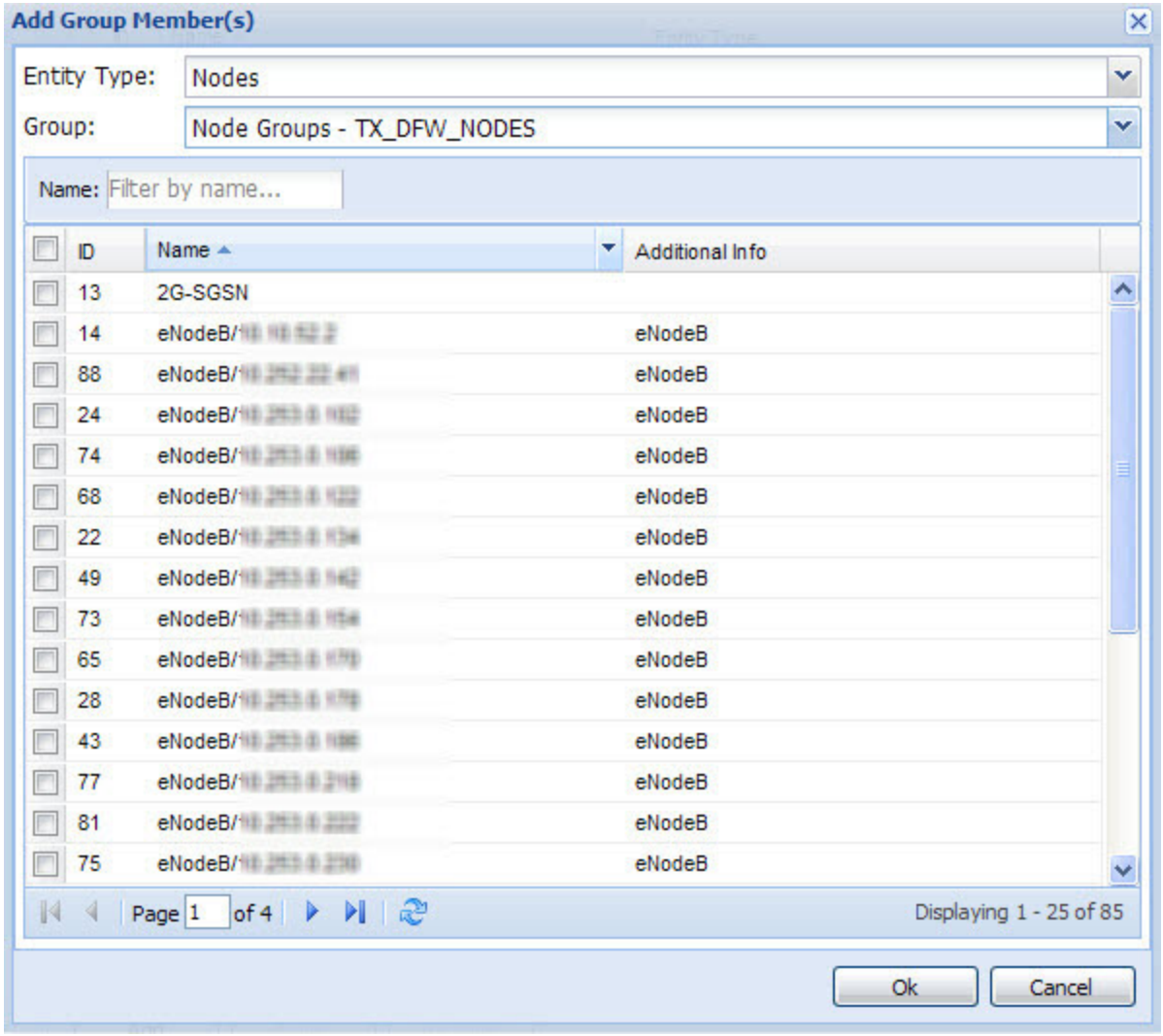
Window Controls

Entity Type Drop-down Menu	Select an Entity Type and Group to view available entities to add to the selected group: Entities will not appear until you make a selection from both drop-down menus. • Select the entity type you want to add to a group. Only physical link groups, node groups, and probe groups are supported in the current release. • Select the group to which you will be adding entities. Group names display in the format [Group Entity] - [Group Name]. Refer to Configuring Entity Groups for details. Entities will not be available for you to select if they: • belong to another group within the same group type. • are already associated with the selected group.
Group Drop-down Menu	
Name Filter Field	Search the group members by name. Enter one or more characters in the element's name and press Enter or Tab. • Filter is not case sensitive • The system searches for all entity names containing the characters you type. • Matching elements appear in the file list.
Members Check Boxes	Select the top check box in the far left column to choose all entities in the list. Or, select specific entities by clicking on their corresponding row check boxes.
OK Button	Apply the changes and close the Group Member(s) dialog box.
Cancel Button	Close the Group Member(s) dialog box without applying changes.
Paging Controls	• Last/Next Page Buttons: Navigate to view entities in multiple pages. • First/Last Page Buttons: Go to the first or last page of the elements list. • Refresh Button: Manually refresh the element list.

Column Filters

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the check mark from columns you want to hide. At least one column must remain visible.

Add Group Members Dialog Box



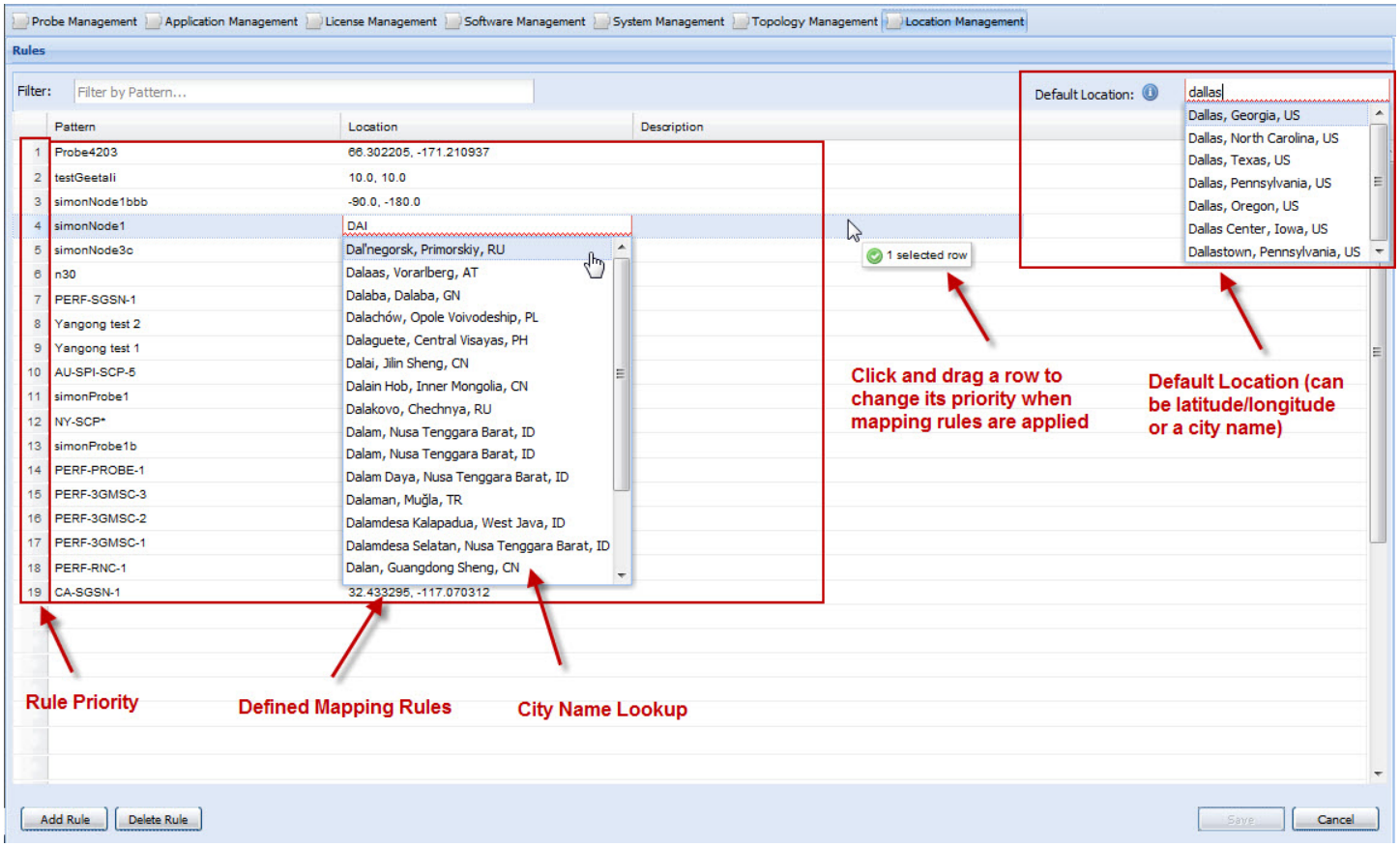
Locations Tab

The Locations tab enables you to define rules for the Iris system to auto-populate locations on Iris Maps (latitude and longitude values) for GeoProbe and Iris nodes and probes based on their names.

Filter	Search the patterns by name. Enter one or more characters in the pattern's name. Filter is not case sensitive. The system searches for all entity names containing the characters you type. Matching elements appear in the file list.
Default Location	Define default location values for your network maps. The values can be latitude and longitude coordinates, or a city name. Elements for which no mapping rules apply are placed at the default location on the map. Valid latitude coordinates are between -90 and 90; valid longitude coordinates are between -179.99 and 179.99. Various Internet sites provide longitude and latitude coordinates when you enter address information.

Pattern Column Location Column Description Column	• Define a location **Pattern** you currently use in element names (see Locations Pattern Definitions for details). • Enter **latitude** and **longitude** values for the location you want to define or enter a partial **city** name to select from a lookup menu. • Valid latitude coordinates are between -90 and 90; valid longitude coordinates are between -179.99 and 179.99. • Lat/Lon values separated by a comma or semi-colon can be copied from a source (such as the Internet) and pasted into the field; Iris automatically separates the values into separate fields. • Define the actual name of the location in the **Description** column. • Click and drag a row to change its priority when Iris applies the mapping rules.
Add Rule	Add a new blank row at the top of the list.
Delete Rule	Delete the selected row.
Save	*NOTE: Depending on your network size and system element types (GeoProbe and Iris), applying the mapping rules to the existing topology could take up to 20 minutes.* • Save mapping rules and apply to all existing GeoProbe and Iris elements that do not have geocodes manually defined (see Node Details Pane or Probe Details Tab). • Iris will also apply the rules when new GeoProbe and Iris elements are configured without geocodes. • All changes are logged by the Iris Activity Log.
Cancel	Cancel your changes and revert to the previously saved settings.

Locations Tab



Locations Pattern Definitions

In the Locations tab, you can define character patterns used in element names that the Iris system can match and assign defined location coordinates. For example, you can define a pattern for all elements having “DAL” in their name so the Iris system assigns the longitude and latitude coordinates for Dallas, Texas, and places these elements in the appropriate location on the map.

Iris supports alphanumeric characters, asterisks (*), and Java regular expressions as shown in the following table.

Characters	Alphanumeric characters, minus (-), underscore (_), period (.), space, colon (:), or forward slash (/) are allowed.
Asterisks (*)	Use an asterisk (*) to replace multiple characters in any part of the keyword. Examples include: • *DAL* • *DAL • DAL* • DAL*1*

Java regular expressions	Any Java regular expression can be used for pattern matching. If you want to use regular expression rather than the simple search mode, you need to enclose them in with "/" (for example, /VP-SS-[12345]/). Refer to Java documentation for comprehensive information about Java regular expressions.
	Examples include:
	• DAL\d - \d represents any digit
	  • Match: DAL01, DAL45, DAL678
	  • No match: DALLAS, DALFW, FWDAL_2
	• DAL\D - \D represents a non-digit
	  • Match: DALLAS, FWDAL_2, DALFW002
	  • No match: DAL01, DAL45, DAL678

Appendix B

Iris User Privileges

After Iris users log on to the Iris system, access to the Iris applications is controlled by role assignment. Each role contains a set of privileges to ensure appropriate access to job-related tasks. The Iris System Administrator assigns defined roles to each user account.

The following table describes the privileges available in Iris. The administrator can add different combinations of privileges to create a role. Users can view their assigned privileges in the User Management User Details window.[1]

Privilege	System Access	Tasks
3rd Party API Access	ISA API	Access the ISA API capability.
Admin Privilege	System Config • Probes tab • Applications tab • Licenses tab • Software tab • System tab • Topology tab • Location tab	All system configuration tasks: • Configure probe settings • Configure physical device ports • Configure disk arrays • Configure Store to Disk settings • Configure XDR profiles • Configure ISA System Default Node Type Order • Manage Probe Software Updates • Configure server settings • Configure Topology entities • Configure element geographical coordinates using the Map Location Editor dialog in the Network Maps application • Use the Session Management tab to attach to or terminate all non-media sessions • Configure Location rules for geographical coordinates
Alarm Acknowledge Privilege	Displays Acknowledge check boxes and ACK button on Alarm Dashboard	• Acknowledge ITA, IPI, KPI Studio, ACE, and system-level alarms

Privilege	System Access	Tasks
Application Alarm Admin Privilege	Alarms Policy Management	For ITA, IPI, KPI Studio, and ACE: • Create new policies • Edit any policy or template, public or private • Delete any policy or template, public or private • Configure system level alarms • Export all policies, action templates, schedule templates, and profiles to an XML file • Import policy configuration files (configuration files contain policies, action templates, schedule templates, and profiles) • Display the content of the XML schema file within the default Internet browser
Application Alarm Configuration Privilege	Alarms Policy Management	For ITA, IPI, KPI Studio, and ACE: • Create new policies • Edit their own policies and templates as well as any designated as public • Delete their own policies and templates as well as any designated as public
Alarm Clearing Privilege	View and access Clear check boxes and CLEAR button on Alarm Dashboard	• Clear ITA, IPI, KPI Studio, ACE, and system-level alarms
Application Alarms on Alarm Dashboard	Alarm Dashboard	• Monitor ITA, IPI, KPI Studio, and ACE alarms
System Alarms on Alarm Dashboard	Alarm Dashboard	• Monitor System-level alarms
Configuration Privilege	System Config • Probes tab • Applications tab • Licenses tab • Software tab • System tab • Topology tab • Location tab	• Configure probe settings • Configure physical device ports • Configure disk arrays • Configure Store to Disk settings • Configure XDR profiles • Configure ISA System Default Node Type Order • Manage Probe Software Updates • Configure Server settings • Configure Topology entities • Configure element geographical coordinates using the Map Location Editor dialog in the Network Maps application • Use the Session Management tab to attach to or terminate all non-media sessions
Conversational Video Privilege	ISA application	• Can analyze captured conversational video and related audio using the ISA Media Player.
DTMF Authorized	ISA application	• Expand DTMF flows in the Results window to analyze packet decodes • View DTMF digits in the DTMF column and Flow Details window

Privilege	System Access	Tasks
IFC Privilege	Not applicable	When an IFC profile runs and is configured to save the artifacts to the remote server repository, the artifacts are stored either in the public or private area for the IFC profile on the repository. All users can see the public area. Users with the IFC privilege can see the private area.
Firmware Administration Privilege	Software tab • By Probe - Firmware tab • Firmware Audit Tab • Campaign Details - Firmware Campaign Type	• View/export firmware audit inventory information on a per-probe basis • View/export firmware audit inventory information for all/selected probes • Create, schedule, and activate Firmware campaigns
IFC Admin Privilege	System Config Configure profiles to schedule session traces for customers of interest, and save them to a local disk or a remote server repository.	• Set up schedule options: start, end, frequency • Determine the monitored objects • List the IMSIs of interest • Determine whether the profiles and sessions are to be stored locally or on a remote server • If stored on a remote server, determine whether the profiles and sessions are to be stored in the private area on the repository or a public area
IPA Privilege	PA application	• Set up capture filters • Run real-time capture sessions • Run historical capture sessions
IPI Privilege	IPI application To launch ISA from within IPI, user must also have the ISA privilege.	• View dashlets • Set filters • Drill-down to any KPI level
ISA Automatic Full MPC	ISA application	Users can enable full MPC for their ISA sessions.
ISA Flow Packet Retrieval	Retrieve User Plane options in ISA application	• Retrieve and view ISA user plane PDUs in ISA Ladder Diagram and PDU Details Pane
ISA G10 Show MOS-CQ Not LQ Privilege	Not applicable	View either MOS-CQ or MOS-LQ values for PDUs in the ladder diagram for G10 probes: • **Enabled (checked)**: View MOS-CQ values • **Disabled (unchecked)**: View MOS-LQ values
ISA Override MPC Rule-sets	ISA	Users can override default ISA MPC correlation rules and choose one or more custom MPC rule sets. Contact Tektronix Communications Customer Support for information about customizing MPC rule sets.
ISA Privilege	ISA application	• Configure capture filters • Start capture sessions • Drill to decode

Privilege	System Access	Tasks
ITA Privilege	ITA application To launch PA from within ITA, user must also have the IPA privilege.	• View dashlets • Set filters • Drill-down to any KPI level
myIrisView Admin Privilege	myIrisView	Users can view, edit, and delete any myIrisView dashboard marked Public or Private. See myIrisView Roles for more information.
Network Maps Privilege	Network Maps application	Users can view Network Maps but cannot make configuration changes to maps.
SMS Full Content Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Allows the viewing of SIP messages including SMS and MSRP content. • **Disabled (unchecked)**: Allows the viewing of SIP messages with user content concealed with asterisks (*).
System Health Customer Privilege	Iris System Health Reports	Users can view and run Iris System Health reports.
User Content Capture Privilege	Not applicable	For ISA: • **Enabled (checked)**: Allows capture of SMS and MSRP content in the G10 probe for use by Iris applications. • **Disabled (unchecked)**: User content concealed with asterisks (*).
User Content Visible Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Allows the viewing of content including SMS and MSRP content. • **Disabled (unchecked)**: User content concealed with asterisks (*).
User Digits Unmasked Privilege	Not applicable	For ISA and PA: • **Enabled (checked)**: Can view user digits such as IMSIs. • **Disabled (unchecked)**: User digits are concealed (masked) with Xs in the system. The Admin can set the number of digits to conceal from 0 to 99 digits in the System Tab.
User Plane Admin Privilege	Media and User Plane Capture functionality within ISA application	• Configure filters to identify media streams to capture in ISA • Capture and monitor real-time media streams in ISA • Analyze captured data using Wireshark • In the Session Management page, view, attach, or terminate media capture sessions created by other users

Privilege	System Access	Tasks
User Plane Capture Privilege	Media and User Plane Capture functionality within ISA application	• Configure filters to identify media streams to capture in ISA • Capture and monitor real-time media streams in ISA • Analyze captured data using Wireshark • Detach captured media sessions so they run unattached
User Plane Analysis Privilege	User Plane export to PCAP and Wireshark functionality within ISA application	Users can export User Plane data to PCAP files and launch Wireshark to view data and play back audio for User Plane flows.
UUMS Admin Privilege	User Management	User management tasks for Admin: • Configure LDAP Server settings • Configure password policy and quality settings • Create roles • Provision users and assign roles Users without the UUMS Admin privilege can only view their user information and currently assigned roles and change their password (Iris LDAP only). This privilege cannot be assigned to any other users.
	Activity Log	• View and filter activity log messages • Export messages to PDF or CSV

[1]User Content Visible and User Digits Unmasked settings can be found on the Subsystem Defaults window for global defaults, and on the User Details pane for individual settings. During migration from version 7.12.1 to 7.12.2, users with the "User Content Visible" and User Digits Unmasked" privileges will retain the settings they had in previous software releases. Users without these privileges will have the default global settings that are configured on the Subsystem Defaults page.

mylrisView Roles

Tektronix Communications provides two predefined user roles for managing and accessing mylrisView, based on the purchasable mylrisView license. You can edit these roles by adding and removing users; however, you cannot add any privileges to the roles or delete either of the mylrisView roles.

The following table describes the mylrisView roles.

Role	Description
MYIRISVIEWADMIN	Users with this role can view, edit, and delete any mylrisView dashboard marked as Public or Private. This is not a licensable role; however, you have to have the MYIRISVIEW_ROLE to access mylrisView.
MYIRISVIEW_ROLE	Users with this role can access the mylrisView application. Users can view any dashboard marked as Public, but can only modify their own mylrisView dashboards. The MYIRISVIEW_ROLE is licensed. You will not be able to assign users to this role if you exceed the number of named users allowed for that license.

Appendix C

Digit and User Content Masking in Iris

Digit and content masking conceals network traffic and call contents from unauthorized access and protects the privacy of customers' personal information. The number of digits masked is a system-wide setting. Contact Customer Support for details.

Digits are masked with the letter X and content is masked with an asterisk (*).

Digit Masking Support

When digit masking is enabled, ISA and PA mask the digits or data elements that can identify the individual parties involved in the call or session. This applies for all protocols which ISA and PA decode. For numerical digits (such as phone numbers, IMSI, and IMEI) the administrator can configure the number of digits that will be masked from the least-significant (right-most) digits. Other digit types, such as URI and user name, are always completely masked.

User Content Masking Support

The following table lists the protocols and services that are supported by user content masking in ISA and PA.

MSRP	MSRP message payload content is masked on G10 probes.
POP3	Entire user content is masked.
SIP	SIP user content is masked. For G10 probes, SMS text content is masked when carried in SIP messages.
SMTP	Entire user content is masked.
SMS	All SMS Text is masked.

Appendix D

This appendix provides example configuration scenarios and the associated Physical Device Port settings in the Probes Tab.

For more information about G10 probe hardware installation and maintenance, refer to the ***G10 Installation Guide*** and the ***G10 Hardware Maintenance Guide***.

Physical Device Port Configuration Examples

This section provides examples for a standalone G10 probe. You configure and modify the probe's physical device ports on the Probe Details tab. For multi-chassis configurations, refer to the appropriate installation guide for that specific probe.

Monitored Link Support

You configure and modify the probe's physical device ports based on:

- Type of G10 interfaces the probe is monitoring (1G or 10G). Monitoring both 1G and 10G interfaces is supported on the same probe in various combinations under the following conditions:
  - Maximum support of 8 total ports (1G + 10G)
  - Maximum support of 4 10G ports
- Whether the monitored network connects to the G10 via span/mirror ports or optical tap/splitters

The following table summarizes the maximum number of monitored links per probe based on interface type and link type.

Interface Type	Link Type	Maximum Monitored Links
Span/Mirrored (1 monitored link requires 1 port)	1G	8
	10G	4
	Mixed 1G + 10G	4 10G + 4 1G max 3 10G + 5 1G max 2 10G + 6 1G max 1 10G + 7 1G max
Optical Taps/Splitters (1 monitored link requires 2 ports)	1G	4
	10G	2
	Mixed 1G + 10G	2 10G + 2 1G max

Refer to the following sections for more information:

- IIC200 Physical Device Port Configuration Examples
- IIC100 Physical Device Port Configuration Examples

IIC200 Physical Device Port Configuration Examples

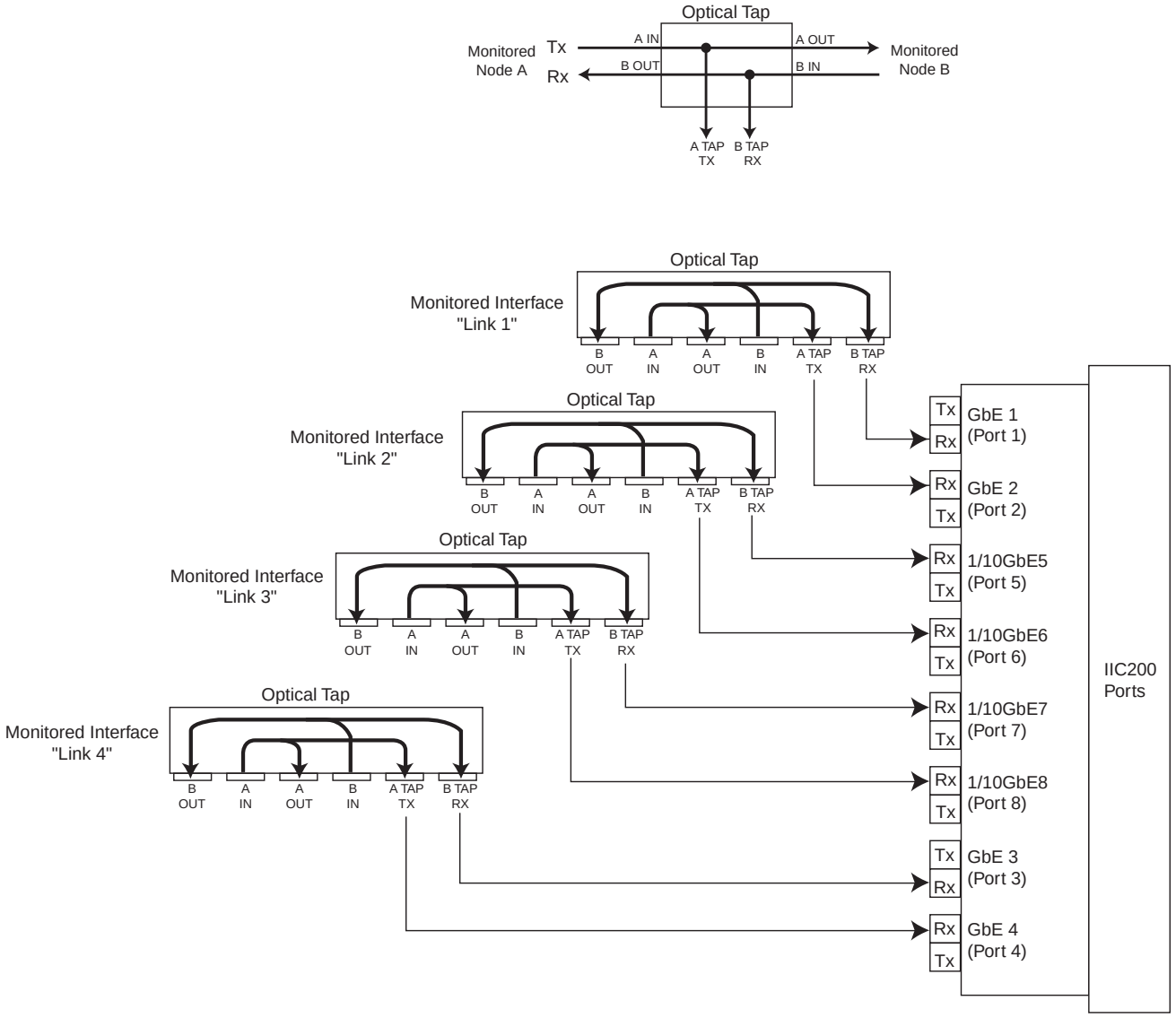
This section provides examples for a standalone G10 probe with an IIC200 configuration. You configure and modify the probe's physical device ports on the Probe Details tab. For multi-chassis configurations, refer to the appropriate installation guide for that specific probe. See also IIC100 Physical Device Port Configuration Examples.

The IIC200 has 8 ports which can be used for 1G Ethernet connections. Ports 5-8 are dual-purpose sockets which can be used for either 1G or 10G Ethernet connections. See Monitored Link Support for details.

Optical Taps/Splitters Ports

The following graphic shows how a monitored network connects to the IIC200 using optical taps or splitters.

- Each optical splitter/tap link requires two physical ports
- A TAP TX connects to one G10 port; B TAP RX connects to a separate G10 port
- Optical splitter/tap links do not use G10 TX ports



8x1G Example

The following table shows the Physical Device Port settings that would be set for an 8x1G example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

Full Duplex is recommended for most configurations; Half Duplex may be required in certain configurations.

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	RX	1	true	false	Full-Duplex	

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
2	Port 2	TX	1	true	false	Full-Duplex	
3	Port 3	RX	1	true	false	Full-Duplex	
4	Port 4	TX	1	true	false	Full-Duplex	
5	Port 5	RX	1	true	false	Full-Duplex	
6	Port 6	TX	1	true	false	Full-Duplex	
7	Port 7	RX	1	true	false	Full-Duplex	
8	Port 8	TX	1	true	false	Full-Duplex	

Mixed Model Example (4 1G and 4 10G)

The following table shows the Physical Device Port settings that would be set for a mixed model (4 1G x 4 10G) example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

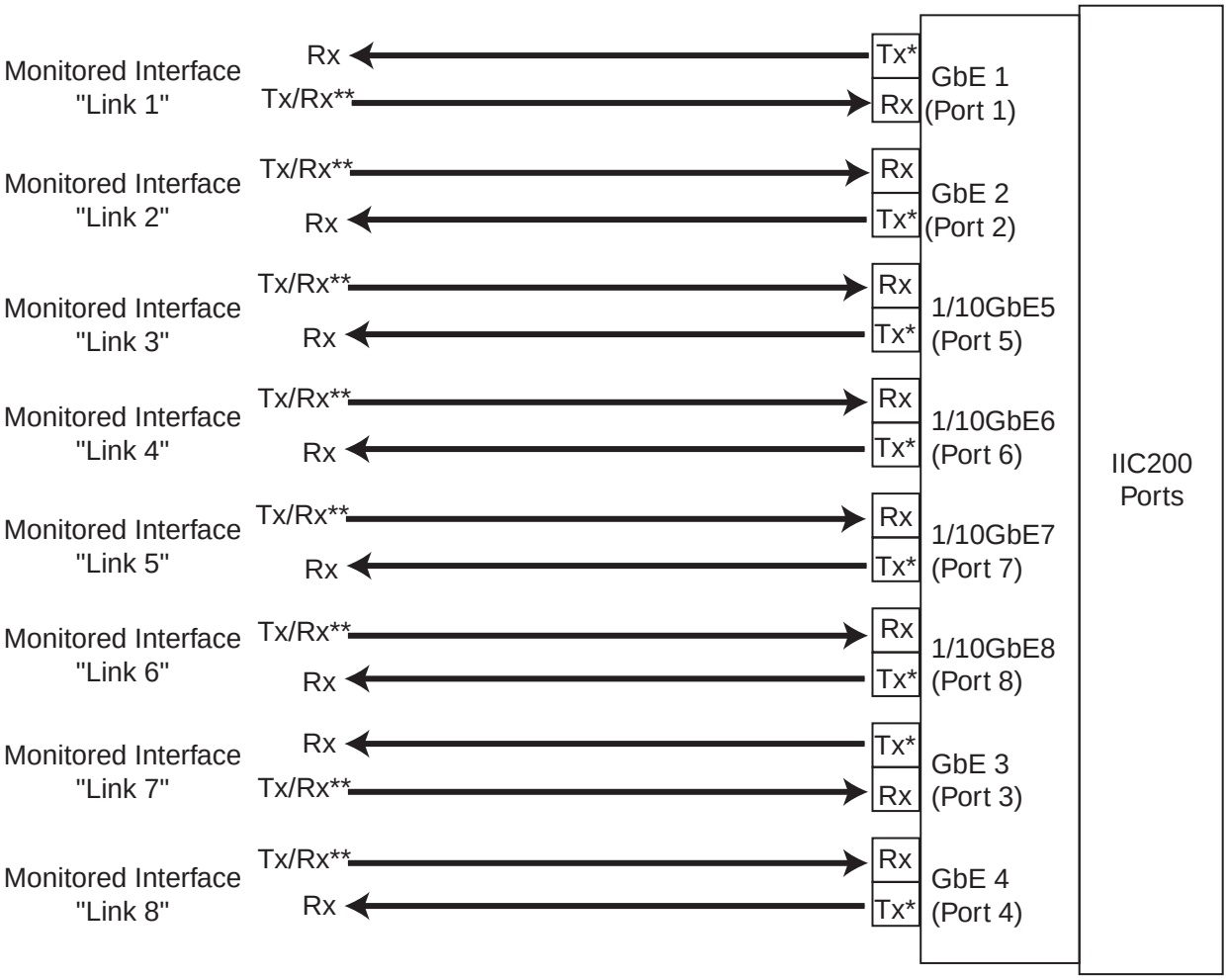
Op Mode is disabled for 10G ports; the Iris system supports only the default Negotiate setting.

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	RX	1	true	false	Full-Duplex	
2	Port 2	TX	1	true	false	Full-Duplex	
3	Port 3	RX	1	true	false	Full-Duplex	
4	Port 4	TX	1	true	false	Full-Duplex	
5	Port 5	RX	10	true	false	Negotiate	
6	Port 6	TX	10	true	false	Negotiate	
7	Port 7	RX	10	true	false	Negotiate	
8	Port 8	TX	10	true	false	Negotiate	

Mirror/Span Ports

The following graphic shows how the monitored network connects to the G10 IIC200 for mirror/span ports.

- The monitored interface transmits aggregated RX and TX data to the G10 RX port.
- The G10 transmits light to the RX port to keep the port active.



* The G10 probe transmits light only to keep port active.

** Aggregated data from customer monitored links.

8x1G Example

The following table shows the Physical Device Port settings that would be set for an 8x1G example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	Span	1	true	true	Negotiate	
2	Port 2	Span	1	true	true	Negotiate	
3	Port 3	Span	1	true	true	Negotiate	
4	Port 4	Span	1	true	true	Negotiate	
5	Port 5	Span	1	true	true	Negotiate	
6	Port 6	Span	1	true	true	Negotiate	
7	Port 7	Span	1	true	true	Negotiate	
8	Port 8	Span	1	true	true	Negotiate	

Mixed Model Example (4 1G and 4 10G)

The following table shows the Physical Device Port settings that would be set for a mixed model (4 1G x 4 10G) example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

Op Mode is disabled for 10G ports; the Iris system supports only the default Negotiate setting.

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	Span	1	true	true	Negotiate	
2	Port 2	Span	1	true	true	Negotiate	
3	Port 3	Span	1	true	true	Negotiate	
4	Port 4	Span	1	true	true	Negotiate	
5	Port 5	Span	10	true	true	Negotiate	
6	Port 6	Span	10	true	true	Negotiate	
7	Port 7	Span	10	true	true	Negotiate	
8	Port 8	Span	10	true	true	Negotiate	

IIC100 Physical Device Port Configuration Examples

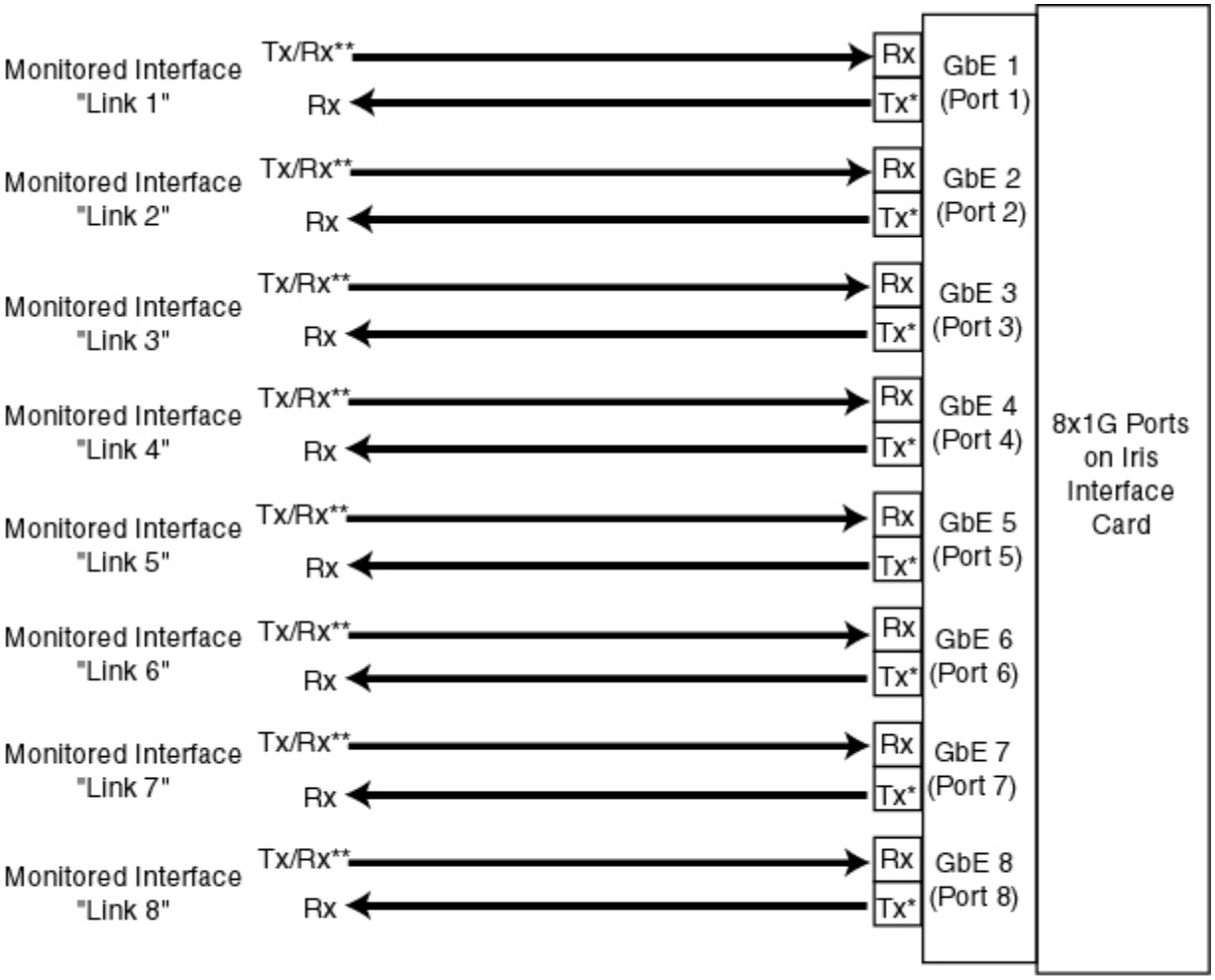
This section provides examples for a standalone G10 probe with an IIC100 configuration. You configure and modify the probe's physical device ports on the Probe Details tab. For multi-chassis configurations, refer to the appropriate installation guide for that specific probe. See also IIC200 Physical Device Port Configuration Examples.

The IIC100 has 8 ports which can be used for 1G Ethernet connections. The TRM100 RTM has 4 ports which can be used for 10G Ethernet connections. See Monitored Link Support for details.

Mirror/Span Ports for 1G

The following graphic shows how the monitored network connects to the G10 1G Ethernet connections for mirror/span ports.

- The monitored interface transmits aggregated RX and TX data to the G10 RX port.
- The G10 transmits light to the RX port to keep the port active.



* The G10 probe transmits light only to keep port active.

** Aggregated data from customer monitored links.

The following table shows the Physical Device Port settings that would be set for this example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

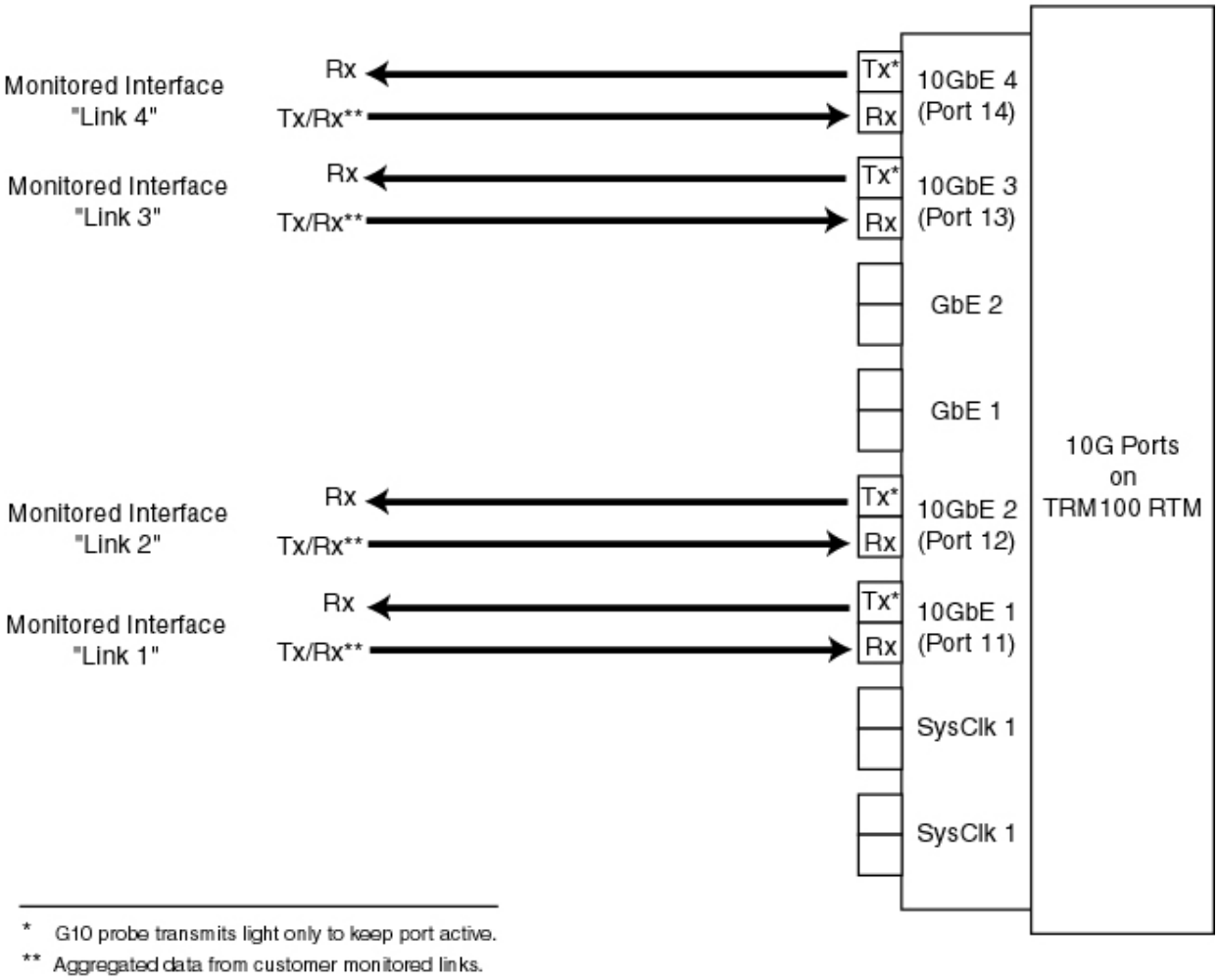
ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	**Port 1**	**Span**	**1**	**true**	**true**	**Negotiate**	
2	**Port 2**	**Span**	**1**	**true**	**true**	**Negotiate**	
3	**Port 3**	**Span**	**1**	**true**	**true**	**Negotiate**	
4	**Port 4**	**Span**	**1**	**true**	**true**	**Negotiate**	
5	**Port 5**	**Span**	**1**	**true**	**true**	**Negotiate**	
6	**Port 6**	**Span**	**1**	**true**	**true**	**Negotiate**	
7	**Port 7**	**Span**	**1**	**true**	**true**	**Negotiate**	
8	**Port 8**	**Span**	**1**	**true**	**true**	**Negotiate**	
9	Port 11	RX	10	false	true	Negotiate	
10	Port 12	RX	10	false	true	Negotiate	
11	Port 13	RX	10	false	true	Negotiate	
12	Port 14	RX	10	false	true	Negotiate	

Mirror/Span Ports for 10G

The following graphic shows how the monitored network connects to the G10's 10G Ethernet connections for mirror/span ports.

- The monitored node transmits aggregated RX and TX data to the G10 RX port.
- The G10 transmits light from the TX port to keep the port active.

If only monitoring two interfaces, connect them to 10GbE 1 and 10GbE 3 to balance the processing load.



The following table shows the Physical Device Port settings that would be set for this example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

Op Mode is disabled for 10G ports; the Iris system supports only the default Negotiate setting.

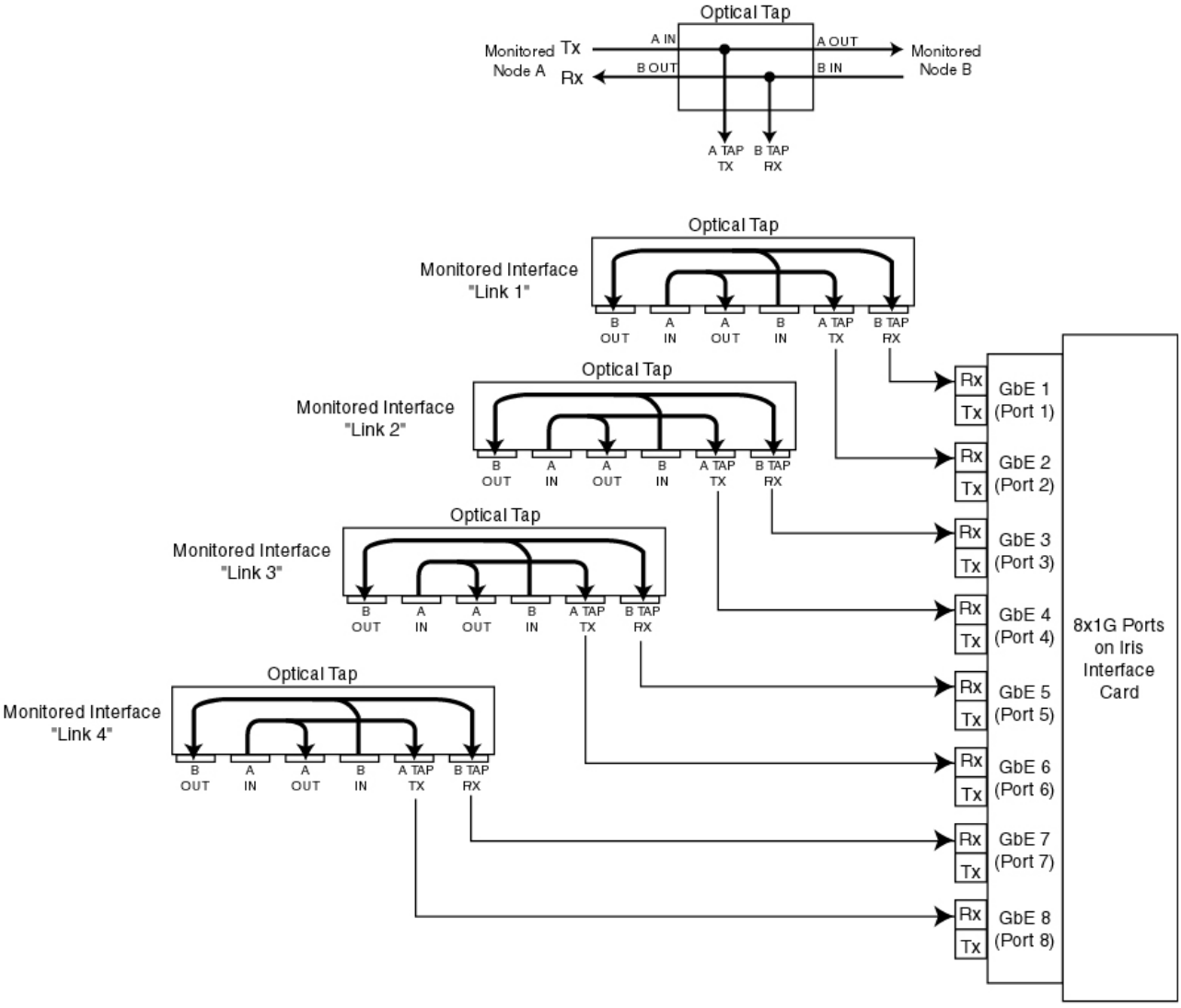
ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	RX	1	false	true	Negotiate	
2	Port 2	RX	1	false	true	Negotiate	
3	Port 3	RX	1	false	true	Negotiate	
4	Port 4	RX	1	false	true	Negotiate	
5	Port 5	RX	1	false	true	Negotiate	

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
6	Port 6	RX	1	false	true	Negotiate	
7	Port 7	RX	1	false	true	Negotiate	
8	Port 8	RX	1	false	true	Negotiate	
9	**Port 11**	**Span**	**10**	**true**	**true**	**Negotiate**	
10	**Port 12**	**Span**	**10**	**true**	**true**	**Negotiate**	
11	**Port 13**	**Span**	**10**	**true**	**true**	**Negotiate**	
12	**Port 14**	**Span**	**10**	**true**	**true**	**Negotiate**	

Optical Tap/Splitter Ports for 1G

The following graphic shows how a monitored network using optical taps or splitters connects to the G10's 1G Ethernet ports.

- Each optical splitter/tap link requires two physical ports
- A TAP TX connects to one G10 1G port; B TAP RX connects to a separate G10 1G
- Optical splitter/tap links do not use G10 TX ports



The following table shows the Physical Device Port settings that would be set for this example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

Full Duplex is recommended for most configurations; Half Duplex may be required in certain configurations.

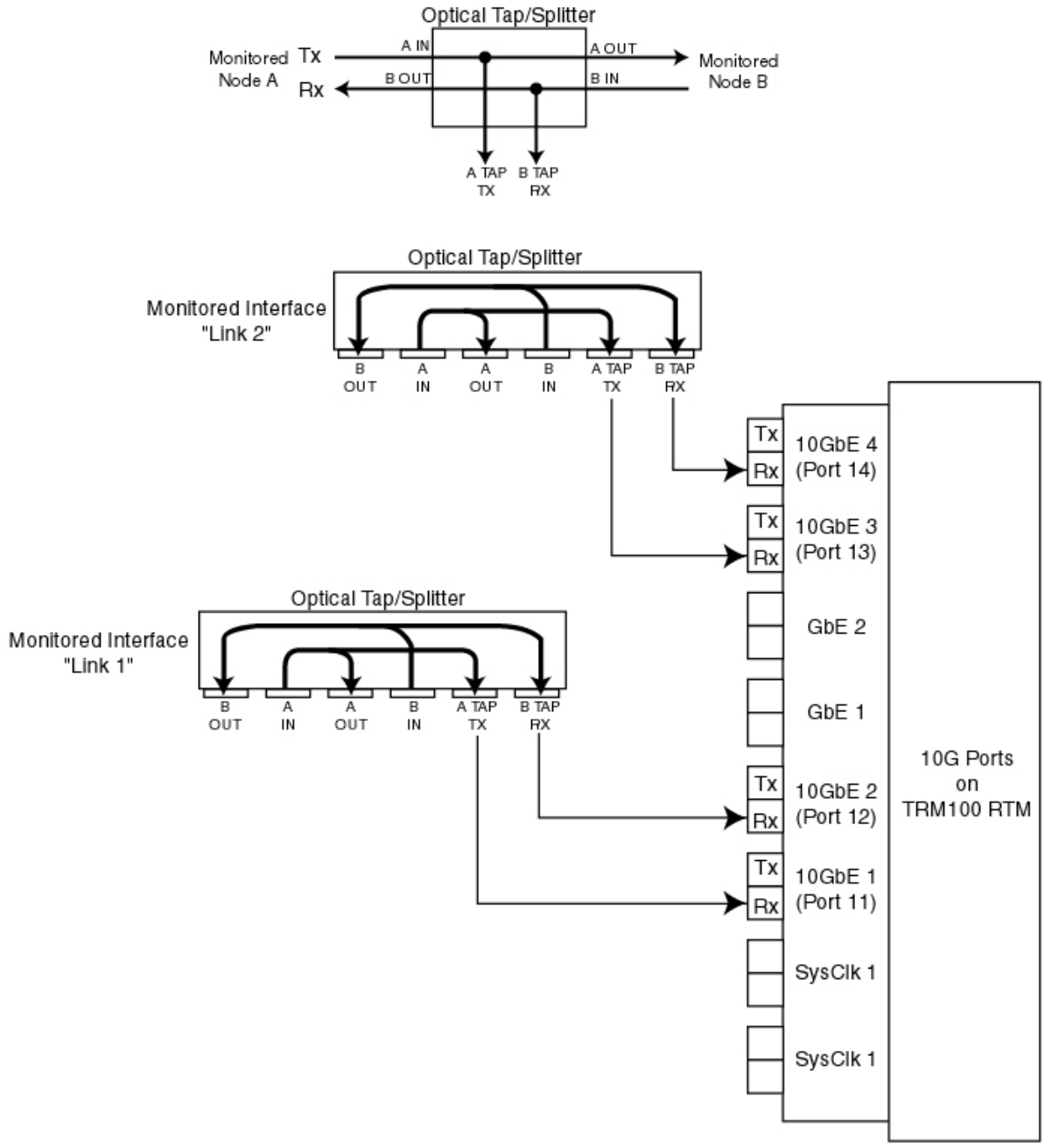
ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	**Port 1**	**RX**	**1**	**true**	**false**	**Full-Duplex**	
2	**Port 2**	**TX**	**1**	**true**	**false**	**Full-Duplex**	
3	**Port 3**	**RX**	**1**	**true**	**false**	**Full-Duplex**	
4	**Port 4**	**TX**	**1**	**true**	**false**	**Full-Duplex**	
5	**Port 5**	**RX**	**1**	**true**	**false**	**Full-Duplex**	
6	**Port 6**	**TX**	**1**	**true**	**false**	**Full-Duplex**	
7	**Port 7**	**RX**	**1**	**true**	**false**	**Full-Duplex**	
8	**Port 8**	**TX**	**1**	**true**	**false**	**Full-Duplex**	
9	Port 11	RX	10	false	true	Negotiate	

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
10	Port 12	RX	10	false	true	Negotiate	
11	Port 13	RX	10	false	true	Negotiate	
12	Port 14	RX	10	false	true	Negotiate	

Optical Tap/Splitter Ports for 10G

The following graphic shows how a monitored network using optical taps or splitters connects to the G10's 10G Ethernet ports.

- Each optical splitter/tap link requires two physical ports
- The A TAP TX connects to one G10 10G port; the B TAP RX connects to a separate G10 10G port
- Optical splitter/tap links do not use G10 TX ports



The following table shows the Physical Device Port settings that would be set for this example. See Configuring Probes for details. The Member Of column will be auto-populated with the name of the physical link to which this port is mapped.

Op Mode is disabled for 10G ports; the Iris system supports only the default Negotiate setting.

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
1	Port 1	RX	1	false	true	Negotiate	
2	Port 2	RX	1	false	true	Negotiate	
3	Port 3	RX	1	false	true	Negotiate	
4	Port 4	RX	1	false	true	Negotiate	

ID	Name	Direction	Gb Capacity	Enabled	TXEnabled	Op Mode	Member Of
5	Port 5	RX	1	false	true	Negotiate	
6	Port 6	RX	1	false	true	Negotiate	
7	Port 7	RX	1	false	true	Negotiate	
8	Port 8	RX	1	false	true	Negotiate	
9	**Port 11**	**TX**	**10**	**true**	**false**	**Negotiate**	
10	**Port 12**	**RX**	**10**	**true**	**false**	**Negotiate**	
11	**Port 13**	**TX**	**10**	**true**	**false**	**Negotiate**	
12	**Port 14**	**RX**	**10**	**true**	**false**	**Negotiate**	

Appendix E

Node Types

This appendix provides a list of available node types within the Iris system. You create nodes using the Topology Tab Nodes feature in Iris Admin.

Note: IPI uses a different set of node types. For a list of IPI node types, see the "IPI Key Performance Indicators" and "IPI Protocols and Interfaces" PDF documents included in the IPI online help.

Type	Definition	Supports	
		IP Addresses	Point Codes
3G MSC	Third Generation Mobile Switching Center	X	
AAA	Authentication, Authorization, and Accounting	X	
AF	Application Function	X	
AS	IMS Application Server	X	
BBERF	Bearer Binding and Event Reporting Function	X	
BSC	Base Station Controller	X	X
BSS	Base Station Subsystem	X	
CDF	Charging Data Function	X	
CRF	Charging Rules Function	X	
CTF	Charging Trigger Function	X	
DNS	Domain Name Server	X	
DRA	Diameter Routing Agent	X	
EIR	Equipment Identity Register	X	
eNodeB	Evolved NodeB	X	
ePCF	Evolved Packet Control Function	X	
ePDG	Evolved Packet Data Gateway	X	
Generic-OnDemand	A general node type that can be configured to represent an individual IP address or group of IP addresses for the purpose of tracking ITA statistics. This node type is only temporarily active for a scheduled time.	X	
GGSN	Gateway GPRS Support Node	X	
GSN NETWORK	GPRS Support Node	X	
HNB-GW	Home Node B Gateway	X	
HSGW	HRPD Serving Gateway	X	
HSS	Home Subscriber Services Node	X	
I-CSCF	Interrogating Call Session Control Function	X	

Type	Definition	Supports	
		IP Addresses	Point Codes
IP Cloud	A device that is configured as a generic IP Node such as a static laptop or mobile IP address.	X	
IP Node		X	
ISDN	Integrated Services Digital Network node	X	
IT Server	A device that provides IT services (such as DNS).	X	
MGC	Media Gateway Controller	X	
MGW	Media Gateway	X	
MME	Mobility Management Entity	X	
MMS	Multimedia Messaging Server	X	
MRF	Media Resource Function	X	
MRFC	Media Resource Function Controller	X	
MRFP	Media Resource Function Processor	X	
MSC	Mobile Switching Center	X	X
MSRP	Message Session Relay Protocol Node	X	
NodeB	The element in a UMTS network that interfaces with the mobile handsets.	X	
OCF	Online Charging Function	X	
OCS	Online Charging System	X	
P-CSCF	Proxy Call Session Control Function	X	
PCEF	Policy Control and Charging Enforcement Function	X	
PCRF	Policy Control and Charging Rules Function	X	
PDF Node	Policy Decision Function	X	
PDN-GW	Public Data Network Gateway	X	
RNC	Radio Network Controller In cases of direct tunnels, user plane traffic can come to GGSNs from RNCs and eNodeBs. Although the G10 does not monitor control plane protocols for these nodes, user plane data coming from these nodes may be seen. You can configure RNCs and eNodeBs so that node names appear in the ISA ladder diagram, not just IP addresses.	X	
S-CSCF	Serving Call Session Control Function	X	
SBC	Session Border Controller	X	
SCP	Service Control Point	X	X
SGSN	Serving GPRS Support Node	X	
SGW	Serving Gateway	X	
SIGTRAN_NODE	Used to represent any SIGTRAN node such as SSP, STP, BSC. Iris categorizes any auto-detected SIGTRAN node with this node type.	X	X
SIP-EP	Session Initiation Protocol Endpoint	X	
SIP-P	Session Initiation Protocol Proxy Server	X	

Type	Definition	Supports	
		IP Addresses	Point Codes
SIP-R	Session Initiation Protocol Redirect Server	X	
Sonus GSX	Sonus Media Gateway	X	
SPGW	Serving Gateway/PDN Gateway	X	
SSP	Service Switching Point	X	X
STP	Signal Transfer Point	X	X
STP/SSP	STP/SSP combination node	X	X
TPF	Traffic Plane Function	X	
Transparent Network Device	Used to represent devices such as routers, gateways, switches, firewalls, optimizers, NAT, media server. Defining an IP address for this node type is optional.	X	
UDR	User Data Repository	X	

Combinational Node Types

Some nodes types such as SGSN, HSS, and EIR are combinational nodes that support Sigtran protocols and pure IP protocols. Iris does not support a single node type for such combinational nodes. The existing SGSN, HSS, and EIR node types as defined in OAM topology are treated as IP nodes. Users cannot assign point codes to these nodes. If Sigtran traffic is detected on a combinational node, and point code(s) are auto-detected, an additional node, with node type of SIGTRAN_NODE is added to topology. This results in one physical node being represented as two separate nodes in Topology.

Appendix F

GTP Split Monitoring Architecture

GTP Monitoring

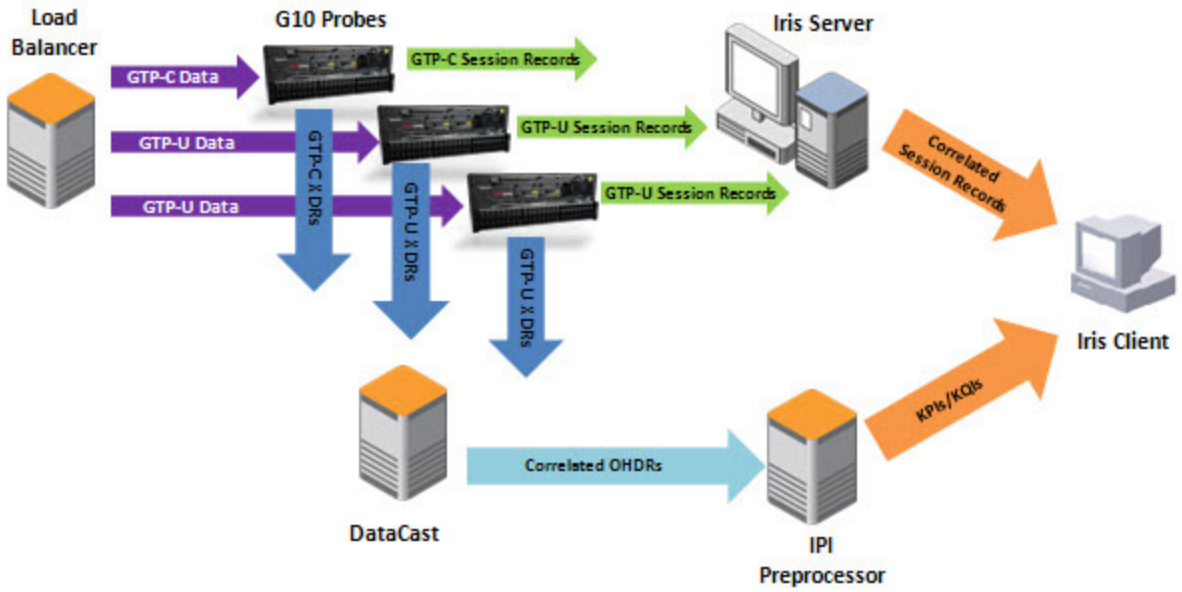
Tektronix' current GTP monitoring solution monitors all GTP user plane (GTP-U) and GTP control plane (GTP-C) traffic belonging to a session using a single probe. This GTP combined monitoring results in a single GTP-C session record/data record (XDR) in which the GTP-U data is included in the GTP-C session record.

Networks continue to expand to support increasing bandwidth demands. Network nodes now support multiple active interfaces with equivalent failover protection interfaces for data transfer; it is no longer guaranteed that traffic for an individual session or flow will be delivered on a single network interface.

To support large networks and allow GGSN scalability, Tektronix offers an alternate G10 architecture that separates GTP-U and GTP-C monitoring for GTPv1 and GTPv2. This GTP split monitoring tracks GTP-C and GTP-U sessions independent of each other (either by separate probes or the same probe) resulting in separate session records. A load balancer ensures that GTP-C and GTP-U data is properly distributed to the appropriate probes.

GTP-C and GTP-U Split Architecture

The following graphic illustrates the split GTP-C and GTP-U architecture.



The following table describes the functions of each network element.

Element	Function
Load balancer	• Forwards GTP-C data to single probe. • Distributes GTP-U data among several probes.
G10 Probes	• Forward GTP-U and GTP-C session records to Iris Server. • Stream GTP-U and GTP-C XDRs to DataCast.

Element	Function
Iris Server	Correlates session records and forwards to ISA.
DataCast	Correlates XDRs and processes them into Output Hybrid Data Records (OHDRs) and forwards them to the IPI preprocessor.
IPI Preprocessor	Processes OHDRs and calculates and aggregates KPIs for use in IPI applications.
Iris Client	• Users view correlated session record results matching their filter criteria in ISA. • Users view KPIs/KQIs in IPI applications and reports.

GTP Combined and Split Monitoring Comparison

The following table summarizes the differences in these types of monitoring.

	Combined	Split
Monitoring	GTP-C and GTP-U monitored together by single probe	• All GTP-C traffic belonging to a session is monitored by the same probe. • GTP-C and GTP-U monitored separately (either by separate probes or same probe).
Session Records/ Data Records (XDRs)	One GTP-C session record/XDR generated per session • GTP-C session record/XDR contains GTP-U data • GTP-C session record/XDRs closed after a configurable period of inactivity (constant GTP-U data keeps the session 'active')	Separate GTP-C and GTP-U session records/XDRs generated per session • GTP-C session records/XDRs remain in memory until they are explicitly closed by 'delete' messages or when probe capacity is reached. • GTP-U session record/XDRs closed after a configurable period of inactivity. • GTP-C and GTP-U session records contain additional data to enable correlation.
Correlation	Correlation not necessary since GTP-C and GTP-U data contained in same session record/XDR	• Iris Session Analyzer (ISA) correlates GTP-C and GTP-U session records using Multi-Protocol Correlation (MPC).[1] • DataCast correlates GTP-C and GTP-U XDR data using the same MPC logic as ISA.
Node Configuration	Optional. If nodes are not configured, the ISA Ladder diagram shows IP addresses instead of node names.	Mandatory for span port configurations. If nodes are not configured, GTP-C and GTP-U data may not correlate correctly for ISA or XDRs.

[1] Correlation of user plane (GTP-U) and control plane (GTP-C) traffic may not always be possible in all cases; for example, if user plane traffic is using a multicast address within the tunnel, an MSIP is not available for the user plane traffic, and therefore cannot be correlated to the control plane traffic.

GTP Split Monitoring in ISA

In GTP Split Monitoring architecture, GTP-U data could be sent from a different probe than its associated GTP-C data. After analyzing GTP-C data in an ISA session trace, if you find that not all GTP-U data is present as expected, perform the following steps for all GTP session traces involving G10 probes:

- Select all G10 probes for GTP session traces
- Always use the Full MPC session trace mode

Enabling GTP Split Monitoring

You enable probes to track GTP-C and GTP-U sessions independent of each other by enabling the "User/Control Plane Split Support" option on the Probes Monitoring Details Tab. You must also configure separate GTP-C and GTP-U XDR profiles and assign them to the relevant probe(s).

Configuring XDRs for GTP Split Monitoring Use Case

Background

For large deployments, G10 probes are configured to support GTP Split Monitoring. In this configuration GTP-C and GTP-U sessions are monitored independent of each other (either by separate probes or the same probe) resulting in separate session records/XDRs. You must configure a separate profile for GTP-C and a separate profile for GTP-U.

Prerequisite

You must enable the "User/Control Plane Split Support" option in the Probes Monitoring Details tab for each probe supporting GTP split monitoring.

To Configure a GTP-C XDR Profile

1. Click the Applications Tab, and select the Traffic Tab.
2. Select GTP or GTPv2 from the Protocol drop-down menu. All defined GTP profiles appear in the XDR Profile List Pane.
3. Click the Add Profile button to add a new profile or the Copy Profile button to copy an existing profile.
4. Enter a name and description for the profile. Make sure to identify this profile as the GTP control plane profile.
5. Enable the profile if you copied an existing profile. New profiles are automatically enabled, you must manually enable a profile you copy.
6. Select the Change option from the Generation Mode drop-down menu. The Change option refers to the keys used for correlation of the control plane and user plane XDRs. When Change is enabled, a GTP-C XDR will be generated for each correlation key change.
7. Define the IP address/port for the DataCast server; these settings must be the same for the associated GTP-U profile.
8. Select the G10 probe that will monitor GTP-C. The GTP-C XDRs will only be generated by one probe; the load balancer ensures that all the GTP-C traffic will be sent to an individual probe.
9. Save the GTP-C profile. If enabled, it is immediately downloaded to the defined probe and GTP-C XDRs are generated based on defined parameters.

   You define white list and black list URLs in a separate GTP-U XDR.

To Configure a GTP-U XDR Profile

1. From the XDR Profile List Pane, select User Plane from the Protocol drop-down menu.
2. Click the Add button to add a new profile or the Copy button to copy an existing profile.
3. Enter a name and description for the profile. Make sure to identify this profile as the GTP user plane profile.
4. Enable the profile if you copied an existing profile. New profiles are automatically enabled, you must manually enable a profile you copy.
5. Select the Closure option from the Generation Mode drop-down menu. GTP-U sessions will be closed after a period of inactivity. The default period of inactivity is 2 minutes, but is configurable (contact Customer Support for details).
6. Define the IP address/port for the DataCast server; these settings must be the same for the associated GTP-C profile.
7. Select the G10 probe(s) that will monitor GTP-U. Selected probes must be in the same load balancer group.
8. Click the Protocol Specific Tab and define white list and black list HTTP URLs.
9. Save the GTP-U profile. If enabled, it is immediately downloaded to the defined probe(s) and GTP-U XDRs are generated based on defined parameters.

Appendix G

Iris Entity Support

Iris applications support entities configured for G10 probes and also entities configured for SpIprobes. The entities you configure on the Topology Tab in Iris Admin are only used by G10 probes. You configure entities for SpIprobes (14U, 3U, and 2U) on the GeoProbe system network maps. Refer to the GeoProbe documentation for configuration details.

Iris entity support varies for each Iris application and depends on whether the entities were configured for G10 probes using the Iris Topology tab in Iris Admin or configured for SpIprobes using the GeoProbe Network Configuration application.

The following table summarizes entity support for each Iris application and each probe type.

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Physical Links • Defined as a bidirectional Ethernet link • Consists of one or more physical ports • Can only be assigned to a single probe	X	X	X	X						
Physical Link Groups • Used to group together one or more physical links • Enables aggregated data display - for example, ITA can display KPIs for a set of links instead of one link at a time • Supports a link belonging to multiple groups		X								

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Logical Links • Concept of logical-level connections in the network, such as IP paths and SCTP connections • Can be grouped at the user-interface level to provide a level of aggregation						X	X	X		X
Logical Link Groups • Used to group together one or more logical links • Enables aggregated data display Supports a link belonging to multiple groups						X	X			X
Nodes • Represents various active network elements with IP addresses such as IT Servers, GGSNs, and SGSNs • Iris and GeoProbe servers are not shown on Maps • Supports individual IP addresses or ranges or point codes • An IP address cannot belong to more than one node		X	X	X	X	X	X	X	X	X

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Node Groups[4] • Used to group together one or more network nodes. • Enables aggregated data to display - for example, ITA can display KPIs for a set of nodes instead of one node at a time • Supports a node belonging to multiple groups		X	X			X	X	X		
Probes • Represents a G10 probe or SpIprobe			X			X		X		X
Probe Groups • Groups one or more probes of the same type			X			X				
G10 Protocols and Applications[5] • Can be enabled or disabled for PDU capture • Supports customizing of L7 application protocol port ranges	X	X	X	X	X					
SpIprobe Protocols • Can be enabled or disabled for PDU capture							X	X	X	
Protocol Groups	Not supported in current release						Not supported in current release			

[1]ISA, PA, and IPI applications require access to historical data stored on G10 probe storage arrays.

[2]Policy Management and ITA do not support SpIprobes.

[3]Applies to policies created for ITA using link, node, and application dimensions, and to policies created for ACE using node dimensions.

[4]IPI supports its own node groups; contact Customer Support for more information.

[5]Refer to the Iris Application System Compliance documents for details about protocol support for specific Iris applications for each probe type.

Appendix H

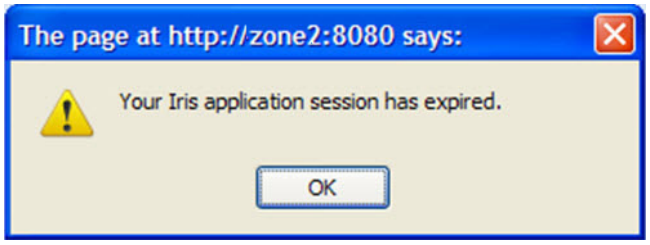
Iris Session Timeouts

The following table describes how the Iris system provides several methods for controlling session timeouts. Call Tektronix Customer Support for assistance when configuring timeout settings.

Timeout	Description	Configuration	Behavior
User Session Inactivity Timeout **Applies to:** All Iris web applications (such as IPI, ITA, Alarms) Does **NOT** apply to ISA and PA applications	A global user session timeout protects Iris server resources by ending an Iris web application session after 30 minutes of inactivity. In some scenarios, users only view Iris applications when monitoring network activity and do not interact with the GUI. The Iris system considers these users inactive after 30 minutes and ends their session (that is, if the application GUI they are viewing is not auto-refreshed).	To avoid sessions from expiring, Tektronix can configure the Iris system to ignore periods of inactivity and keep sessions open until the user logs out. **Advanced Property:** com.tektronix.iris.server.system **Parameter:** isSessionKeepAliveEnabled **Default:** Disabled *The 30 minute value is an Iris system setting and is not configurable.*	**Session Keep Alive Disabled (default)** If a web application is not auto-refreshed, after 30 minutes of user inactivity (**excluding** ISA and PA): • User receives message, "Your Iris application session has expired" • User will either be redirected to the Iris home page to start another session, or if reauthentication is required (Single Sign-on timeout expired), they will be redirected to the Iris login page. **Session Keep Alive Enabled** • User does not receive expiration notice within a web application. • For security purposes, UUMS sessions will continue to expire after 30 minutes of inactivity, even if the Iris system is configured to ignore user inactivity. • **Before enabling this functionality, ensure that it does not violate the customer's security requirements.**

Timeout	Description	Configuration	Behavior
Single Sign-on Timeout **Applies to:** All Iris user sessions **except** ISA and PA	You can configure the number of hours users will remain authenticated after initial login.	**Parameter:** Single Sign-on Timeout field in UUMS Configuration tab; refer to the UUMS online help for details. **Default:** 2 hours	User will only be prompted for username and password during initial login and will not have to reauthenticate by logging back into the system again for the configured time. Note that the user is not logged out if the Single Sign-on timeout expires and he stays on the same web application tab; he will only be prompted for reauthentication if the timeout expires and if he clicks the tab of a different web application for which a session does not already exist. Single Sign-on Timeout does not apply to ISA and PA; users of these applications do not require reauthentication.
ISA Session Idle Timeout **Applies to:** ISA	A timeout can be set to protect probe resources due to inactive ISA sessions.	Tektronix configures this advanced property. **Advanced Property:** com.tektronix.iris.server.system **Parameter:** userSessionIdleTimeout **Default:** 30 minutes	Varies depending on scenario; refer to ISA Session Idle Timeout for details.
PA Session Idle Timeout **Applies to:** PA	A timeout can be set to protect probe resources due to inactive PA sessions.	Tektronix configures this advanced property. **Advanced Property:** com.tektronix.iris.server.system **Parameter:** userSessionIdleTimeout **Default:** 30 minutes	Varies depending scenario; refer to PA Session Idle Timeout for details.

User Session Inactivity Timeout Message



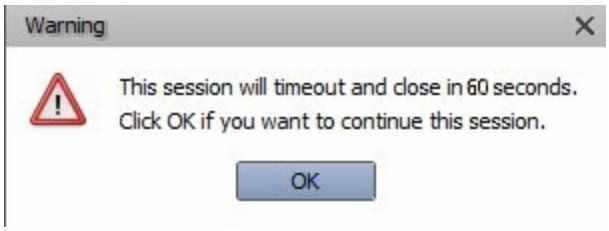
ISA Session Idle Timeout

ISA includes a configurable session idle timeout function with a default of 30 minutes; for changes, contact Tektronix Communications Customer Support . If an ISA session is inactive for the configured timeout value, the ISA Results window closes, and a warning message appears above the ISA Network page stating the session will end in 60 seconds if you do not click OK. If you do not click OK, ISA closes the session and displays a warning message explaining that the session has

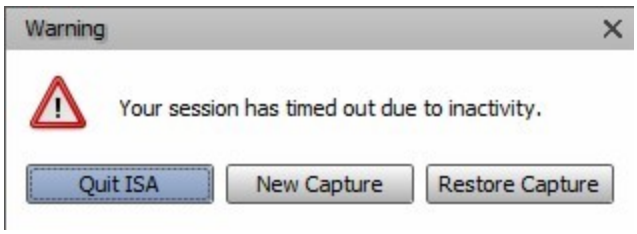
closed due to an inactivity timeout. You can then choose to start a new capture or restore your current capture and its settings.

Session Timeout Options	Description
Quit ISA	Close ISA.
New Capture	Clear all previous selections in the ISA Network page , ISA Filter Builder, and ISA Duration page.
Restore Capture	Keep the ISA Network page open so you can restart the previously closed session with the same settings.

Session Timeout Warning Message



Session Timed Out Warning Message with Options



ISA Session Idle Timeout Scenarios

An ISA Session Idle inactivity timeout can only occur on the ISA Results window. It can happen while sending PDUs to Wireshark when a session is stopped or paused, but it cannot occur while ISA is saving or exporting PDUs to files. The potential for a session idle timeout does not apply to every stage of every ISA session. The following table shows the potential for session idle timeout by session stage and type.

Session Type	Session Stage	Timeout Possible	Restore Session
Historical Capture Session	Session not started	No	No
	Session started and all records/PDUs retrieved	Yes	Yes
	Session started and all records/PDUs not retrieved	Yes When the Resume button is enabled, which means some records have not been retrieved.	No
	Session stopped.	Yes	Yes
Real-Time, Real-Time plus Historical Capture	Any stage	No	No
File Recall Session	Any stage	No	No

PA Session Idle Timeout

PA includes a session idle timeout function that Tektronix Communications Customer Support configures. If a PA session is in a state where probe resources are occupied but not in use and are inactive for the configured amount of time, a warning message appears stating the session will end in 30 seconds if you do not click OK.

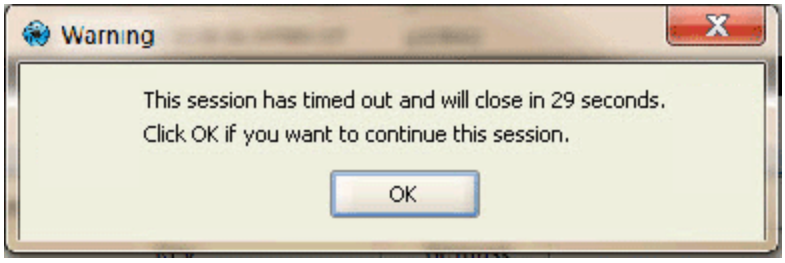
If you do not click OK, PA closes the session to release the probe resources for the benefit of other users. A message appears displaying three options:

- New Session - start a new session
- Restore Session - restore the last session
- Quit PA

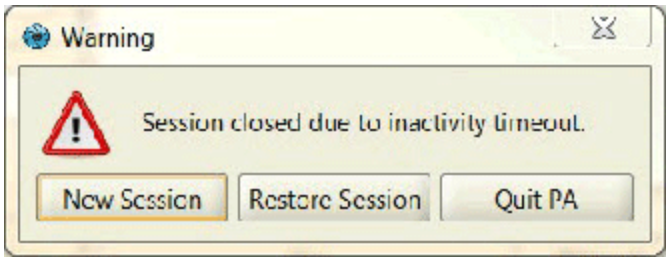
The message also explains that the session was closed due to an inactivity timeout (see Session Idle Timeout table).

If you choose to restore the previous session, both the Real Time and Historical sessions will be restored as an historical session, and will be started automatically. The restored session will include the previously closed capture session setting in the Session Management pane, as well as the previous Capture, Display, and Find filter settings

Client Session Warning Message



Timeout Warning Message



PA Session Idle Timeout Scenarios

The inactivity timeout can only occur on the PA main window. It can occur while sending PDUs to Wireshark, but it cannot occur while PA is saving or exporting PDUs to files. The session idle timeout does not apply to every stage of every PA session. The following table shows the possible occurrence of session idle timeout per session type and stage of session.

Session	Stage of Session	Session Idle Timeout Possible	Restore Session
Real-Time and Historical Capture Session	Session is not applied.	No	Not applicable.
	Session is applied but not started.	Yes	Restore applied session with selected elements.
	Session is started (capture session is ongoing).	No	Not applicable.

Session	Stage of Session	Session Idle Timeout Possible	Restore Session
	Session is stopped but not closed.	Yes	• If the PDU is received, the Restore Session will use last PDU time as the end time. • If no PDU is received and you stop the session: the Restore Session will use the stop time as the end time.
	Session is paused.	Yes	• If no PDU is received and you pause the Session, the Restore Session will use pause time as the end time. (If there are several pauses, PA will use the last pause time).
File Recall Session	Saved file is opened	No	Not applicable.

Appendix I

Iris Server Backup and Restore Utility

Overview

The Iris Server Configuration Backup and Restore Utility provides a reliable way for you to perform scheduled backups of your Iris server's configuration, or restore the configuration from a previously saved version in case of a failure. This utility resides on the Iris server(s) and is driven by UNIX shell commands.

The Iris Server backup and restore utility backs up the part of the Oracle database that supports the Iris nonprobe servers, including but not limited to, these servers: DataCast, IPI Preprocessor, OAM, Oracle, ISA, and ITA. It backs up the configuration information that is needed to bring the Iris servers back to a working state.

For this reason, it is important to follow your IT network best practices to back up your file system frequently and regularly. In the case of a failure, the following is the high-level Iris configuration restoration sequence:

- Restore the server's file system. Follow your IT network process.
- If the Oracle server has failed, install the database software on the database server.
- Run the utility restoration script.

After restoration, these components are restored to their previous state:

- All Tektronix software
- The Iris system configuration
- Users and user preferences and roles
- Alarm definitions
- Saved reports

Application-generated data, such as the following, is not backed up and restored:

- Iris Key Performance Indicators (KPIs)
- Data record (DR) logs
- Generated alarms

After system restoration, the Iris server begins generating new data.

Backup and Restore Operation

The backup and restore process is based on the following:

- UNIX file system backups: Use your IT networking best practices to back up the file system.
- Scheduled configuration backups: The utility permits one instance only per machine to run at the same time. You can configure the backup start time and an offset to define how often the Iris configuration backup runs.
- Multiple servers: The utility supports restoring multiple servers, which means that you can run the restore utility on each server targeted for restoration.
- Maintenance of host name and Iris server version: Restoration depends on the host name and the Iris server version remaining the same. Restoring to a host name or server version that is different from the original host name or server version is not supported.
- The utility restores the Iris configuration to the exact software version that was running before the failure.

- Backup and restoration error messages: You can configure notification of errors, including which action failed, through email alerts.
- Restoring the utilities: Because utilities are installed with the Iris installer, your IT department must have restored the UNIX file system. This restoration necessitates that the Tektronix software binaries, including the utility, are located in their original locations on the UNIX file system.

Estimated Times for Backing Up and Restoring

The estimated times for backing up and restoring can vary considerably. If the Iris servers are deployed on the recommended platforms, you can use the following times for backing up and restoring the configuration as approximations, although the processes can take longer:

- Exporting data for scheduled backups: 30 minutes
- Restoring configuration data: 60 minutes