



# IntraVUE User Manual

Release 1

Issue 1

Copyright © 2018 Panduit Corp. All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from Panduit. No patent liability is assumed with respect to the use of the information contained herein.

Although every precaution has been taken in the preparation of this book, Panduit assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

## Table of Contents

---

<b>Table of Contents</b>	<b>3</b>
<b>IntraVUE Help Navigation</b>	<b>10</b>
How to use the documentation	10
Conventions	11
<b>Getting Started</b>	<b>13</b>
Overview of IntraVUE	13
Installation & Registration	20
IntraVUE Analytics	42
Creating Plant Documentation	53
<b>Import &amp; Export Functions - CSV File</b>	<b>55</b>
Completing Initial Configuration	65
<b>Advanced</b>	<b>90</b>
<b>Administration</b>	<b>91</b>
<b>IntraVUE Architecture</b>	<b>92</b>
<b>New Installation</b>	<b>95</b>
<b>Selecting The Top Parent</b>	<b>99</b>
<b>Installation &amp; Setup</b>	<b>103</b>
<b>User Functions</b>	<b>104</b>
<b>Accessing IntraVUE™ remotely via any Internet Browser</b>	<b>105</b>
<b>First Login</b>	<b>106</b>
<b>Topology View</b>	<b>107</b>
<b>Navigation Menu</b>	<b>115</b>
<b>IntraVUE Legend</b>	<b>117</b>

---

---

<b>Search Devices .....</b>	<b>123</b>
<b>Event Logging .....</b>	<b>125</b>
<b>Event Type Filter .....</b>	<b>128</b>
<b>Selection Criteria and Network Filter .....</b>	<b>129</b>
<b>Device Filter .....</b>	<b>130</b>
<b>Device Side View .....</b>	<b>132</b>
<b>Connection Side View .....</b>	<b>133</b>
<b>Switch Side View .....</b>	<b>136</b>
<b>Selection .....</b>	<b>137</b>
<b>View Filters .....</b>	<b>138</b>
<b>Diagnostics View .....</b>	<b>141</b>
<b>Roaming Devices .....</b>	<b>144</b>
<b>Admin Functions .....</b>	<b>145</b>
<b>Side View in Edit Mode .....</b>	<b>146</b>
<b>Device Configure - General .....</b>	<b>148</b>
<b>Device Configure - Other Names .....</b>	<b>151</b>
<b>Device Configuration - Image .....</b>	<b>153</b>
<b>Device Configuration - Advanced Tab .....</b>	<b>155</b>
<b>Device Configure - SNMP .....</b>	<b>164</b>
<b>Device Configure - Links .....</b>	<b>166</b>
<b>Configure Menu .....</b>	<b>168</b>
<b>Configure Menu - Registration .....</b>	<b>169</b>
<b>Configure Menu - Database Tab .....</b>	<b>171</b>
<b>Configure Menu - Scanner Tab .....</b>	<b>175</b>
<b>Configure Menu - Email Tab .....</b>	<b>180</b>

---



---

<b>Configure Menu - General Tab .....</b>	<b>186</b>
<b>Configure Menu - Advanced Tab .....</b>	<b>188</b>
<b>Admin Verification in IntraVUE 3 .....</b>	<b>195</b>
<b>Adding Users and Changing Admin Password .....</b>	<b>197</b>
<b>VM Host, Hub, or Non-SNMP Switch .....</b>	<b>201</b>
<b>Utility Programs .....</b>	<b>204</b>
<b>User Defined Fields .....</b>	<b>207</b>
<b>Server .....</b>	<b>208</b>
<b>IntraVUE File System .....</b>	<b>209</b>
<b>Predispose.txt File .....</b>	<b>210</b>
<b>The IntraVUE folder .....</b>	<b>211</b>
<b>Backing up files not in the MySql database backup file .....</b>	<b>213</b>
<b>The ivserver.properties File .....</b>	<b>214</b>
<b>Special Files in IntraVUE .....</b>	<b>215</b>
<b>Modbus - TCP and SNMP Data Configuration .....</b>	<b>218</b>
<b>Ping or Connection status .....</b>	<b>219</b>
<b>Disabling Modbus TCP .....</b>	<b>220</b>
<b>Handling Trunking in Switches .....</b>	<b>221</b>
<b>The 'trunkingdefs.txt' File .....</b>	<b>222</b>
<b>Customizing the email message .....</b>	<b>224</b>
<b>VLANs - Virtual Local Area Networks .....</b>	<b>225</b>
<b>How to Add an additional web server Port Number .....</b>	<b>226</b>
<b>IntraVUE Logs .....</b>	<b>228</b>
<b>IntraVUE Appliance .....</b>	<b>230</b>
<b>Using the IntraVUE Appliance as an Agent .....</b>	<b>231</b>

---

---

<b>Using the IntraVUE Appliance as a Server .....</b>	<b>236</b>
<b>IntraVUE Appliance Configuration .....</b>	<b>237</b>
<b>IntraVUE Discovery Tool .....</b>	<b>243</b>
<b>Accessing the appliance in networks having DHCP .....</b>	<b>243</b>
<b>Using the Discovery Tool Utility to Configure the Appliance .....</b>	<b>245</b>
<b>Updating the IntraVUE Appliance Image .....</b>	<b>246</b>
<b>Creating Plant Documentation .....</b>	<b>248</b>
<b>Export / Import .....</b>	<b>249</b>
<b>Import &amp; Export Functions - CSV File .....</b>	<b>252</b>
<b>CSV Column Values .....</b>	<b>256</b>
<b>IntraVUE Diagnostics .....</b>	<b>257</b>
<b>Threshold Graphs .....</b>	<b>258</b>
<b>Multiple Device Side View .....</b>	<b>263</b>
<b>Generate Support Archive .....</b>	<b>265</b>
<b>Event Log Descriptions .....</b>	<b>267</b>
<b>IntraVUE Diagnostics .....</b>	<b>269</b>
<b>KPI Supervisor (IntraVUE™ Advanced Analytics) .....</b>	<b>293</b>
<b>KPI Supervisor .....</b>	<b>295</b>
<b>Installation .....</b>	<b>296</b>
<b>IntraVUE™ Key Performance Indicators .....</b>	<b>298</b>
<b>KPI Supervisor Configuration .....</b>	<b>299</b>
<b>KPI Supervisor Reports .....</b>	<b>303</b>
<b>Current KPI View .....</b>	<b>304</b>
<b>Historical KPI View .....</b>	<b>308</b>
<b>List View .....</b>	<b>311</b>

---

<b>Adding KPI Comments .....</b>	<b>314</b>
<b>Additional Resources .....</b>	<b>316</b>
<b>Technotes .....</b>	<b>317</b>
<b>Keeping Track of Port Speeds .....</b>	<b>318</b>
<b>Identifying Auto-Negotiation issues .....</b>	<b>320</b>
<b>Conclusion: .....</b>	<b>320</b>
<b>Understanding Spikes In Networks .....</b>	<b>321</b>
<b>Wireless Devices Preserving Old Data .....</b>	<b>324</b>
<b>Limiting VLANs on Cisco Switches .....</b>	<b>326</b>
<b>Verifying SNMP on Fully Managed Switches .....</b>	<b>327</b>
<b>NA Nodes .....</b>	<b>331</b>
<b>Supported Protocols .....</b>	<b>335</b>
<b>Device (DLR) and Switch Level Ring Networks .....</b>	<b>337</b>
<b>IntraVUE Agent - Low Cost Agent .....</b>	<b>340</b>
<b>Deploying an IntraVUE™ Agent .....</b>	<b>341</b>
<b>Windows ARP Bursts .....</b>	<b>342</b>
<b>Vendor Name from OUI .....</b>	<b>344</b>
<b>Device Discovery &amp; Management .....</b>	<b>345</b>
<b>SMS Notifications .....</b>	<b>349</b>
<b>View Databases Offline .....</b>	<b>350</b>
<b>HTTPS .....</b>	<b>351</b>
<b>Using HTTPS .....</b>	<b>356</b>
<b>Importing Device Names From Third Party Sources .....</b>	<b>358</b>
<b>Solutions .....</b>	<b>361</b>
<b>Can't view IntraVUE remotely .....</b>	<b>362</b>

---

<b>White screen after upgrade .....</b>	<b>363</b>
<b>Mysql service not being installed by the intravue installer .....</b>	<b>365</b>
<b>Can Intravue scan Profibus networks? .....</b>	<b>367</b>
<b>How to print the Intravue topology from a plotter? .....</b>	<b>368</b>
<b>Cisco Switches with IPDT Cause Duplicate IPs .....</b>	<b>369</b>
<b>Known Issues .....</b>	<b>373</b>
<b>FAQs .....</b>	<b>378</b>
<b>GENERAL FAQs .....</b>	<b>378</b>
<b>INSTALLATION AND SYSTEM REQUIREMENTS FAQs .....</b>	<b>378</b>
<b>CONFIGURATION QUESTIONS .....</b>	<b>379</b>
<b>DIAGNOSING NETWORK ISSUES .....</b>	<b>379</b>
<b>MySQL .....</b>	<b>379</b>
<b>IntraVUE™ AND SYNAPSENSE .....</b>	<b>380</b>
<b>Modbus/TCP .....</b>	<b>380</b>
<b>PLUG AND APPLIANCES FAQs .....</b>	<b>380</b>
<b>INTRAVUE &amp; JAVA FAQs .....</b>	<b>380</b>
	<b>380</b>
<b>INTRAVUE THRESHOLD FAQs .....</b>	<b>380</b>
<b>KNOWN SWITCH ISSUES FAQs .....</b>	<b>381</b>
<b>GENERAL FAQs .....</b>	<b>381</b>
<b>INSTALLATION AND SYSTEM REQUIREMENTS FAQs .....</b>	<b>389</b>
<b>CONFIGURATION QUESTIONS .....</b>	<b>391</b>
<b>DIAGNOSING NETWORK ISSUES .....</b>	<b>396</b>
<b>MySQL .....</b>	<b>403</b>
<b>IntraVUE™ AND SYNAPSENSE .....</b>	<b>405</b>

---

---

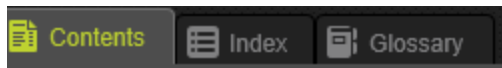
<b>Modbus/TCP .....</b>	<b>405</b>
<b>THRESHOLD (PING, PING FAILURES, BANDWIDTH) FAQs .....</b>	<b>406</b>
<b>PLUG AND APPLIANCE FAQs .....</b>	<b>406</b>
<b>INTRAVUE &amp; JAVA FAQs .....</b>	<b>410</b>
<b>INTRAVUE THRESHOLD FAQs .....</b>	<b>412</b>
<b>KNOWN SWITCH ISSUES FAQs .....</b>	<b>412</b>
<b>Topology View .....</b>	<b>416</b>
<b>Glossary .....</b>	<b>424</b>
<b>Index .....</b>	<b>439</b>

## IntraVUE Help Navigation

■

### How to use the documentation

The IntraVUE online help is the best place to find information about usage and settings of the IntraVUE Network Visualization and Analytics tool. To navigate better when using this online help system, please take a moment to review these points.




**Contents** - This tab contains a table of contents of all learning materials broken down into sections for you to browse.

**Index** - This tab contains the specific topics in alphabetical order for easy look up and access.

**Glossary** - This tab contains technical terms meaning and acronyms commonly used by IntraVUE and throughout Industrial Automation environments.



**Print** - Allows you to print the topic currently displayed on the right pane of the browser.

**Expand all/ Collapse all** - Click this when you want to see hidden information, specifically, when this icon  appears.

**Highlight** - Allows you to remove highlighting of keywords after performing a search.



**Search** - Allows you to search for keywords or specific topics. You can perform on various sections of the online help system including:

1. All Files
2. Articles

- 3. Downloads
- 4. Introduction Topics
- 5. Popular Content



**Navigate previous / Navigate next** - Click each arrow to move back and forth from one topic to another in chronological order in the Contents tab.

## Conventions

This guide contains seven types of notes. Each note type is described below.



**Warning** notes help you avoid mistakes that may result in database corruption, data loss, abnormal behavior, or other unintended results inside IntraVUE™.



**Caution** notes help you avert a mistake but are not as critical as warnings. These notes can also describe a result that may not be obvious to you after a configuration or device change.



**Recommended** notes indicate a section that contains a best practice, or a recommended process or method that you should follow to improve performance or efficiency of IntraVUE™.



**Tips** provide helpful hints or shortcut to a feature or functionality.



**Save** appears when saving your work for system configurations or any other change is recommended.



**Notes** calls attention to information that may otherwise get lost in text or hard to identify (e.g. configuration sub-setting).

**IntraVUE™**  
Information is  
below

---

**Collapsed Sections** will be hidden when you visit the page. Click this button to expand it.

**Network Scanner**<sup>1</sup> **Glossary Terms** will appear in blue text. When you hover over them, the definition on the word or phrase displays in a pop-up window.

## Contacting us

If you find an error or want to suggest enhancements to our documentation, please provide the following information in your correspondence. If you would like a response to your correspondence, include your name and email address as well.

- » For PDFs, include the title of the document, the section heading, and the page number.
- » For online documentation, include the heading of the page or the breadcrumbs from the top of the page (for example, Advanced > IntraVUE Analytics > Device Threshold Line Graphs).

Contact options.

- » Email us at [techsupport@panduit.com](mailto:techsupport@panduit.com).

Thanks for helping us improve our documentation.

---

<sup>1</sup>Continuously monitors the configured networks checking for device disconnections, new devices added, and threshold data from SNMP MIB data fields. The scan engine uses Ping and ARP to detect the presence of devices and SNMP to get information about the hierarchy of the network. This information is stored in the database.

---



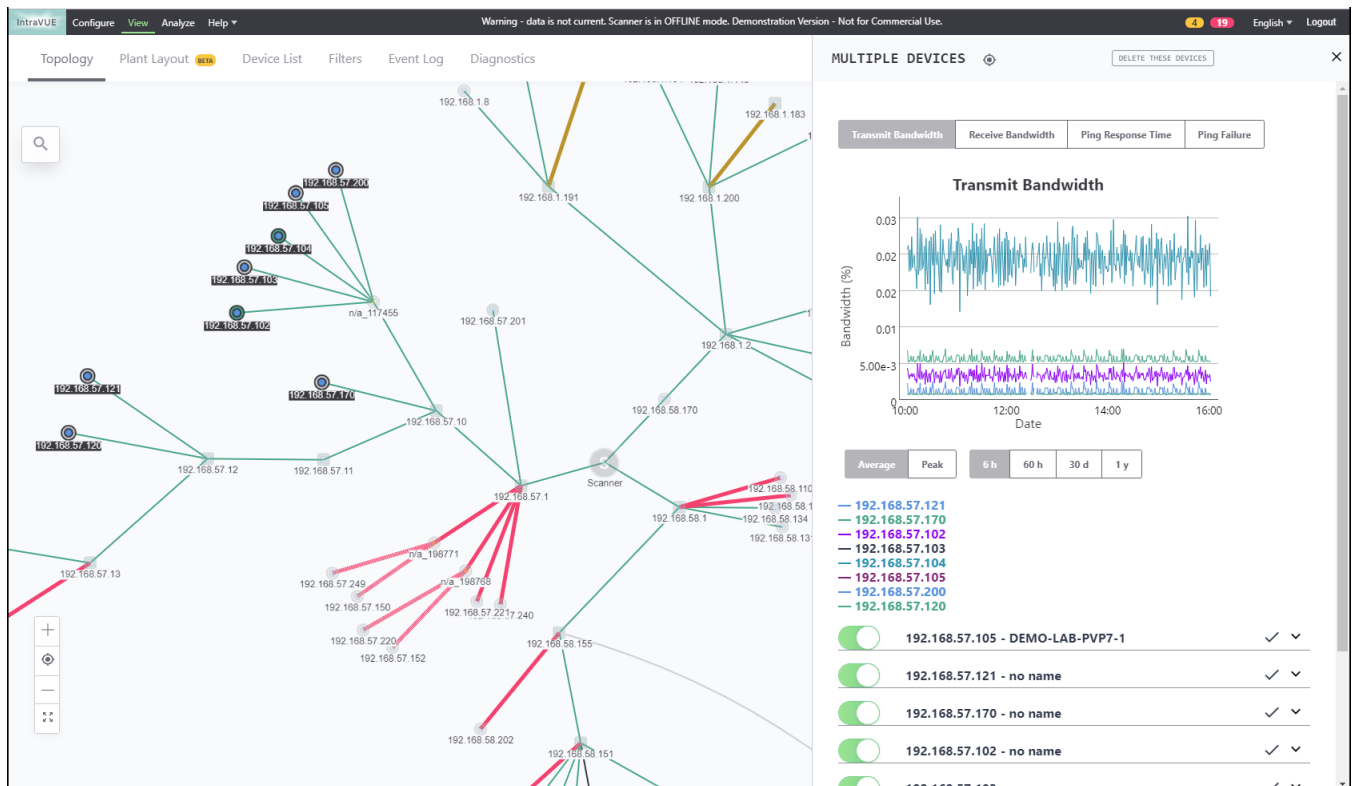
## Getting Started

### Overview of IntraVUE

IntraVUE is a network Visualization, Documentation, Diagnostics, and Analytics platform for current and future needs of IIoT (Industrial IoT), and Industrie 4.0.

Installed as a web server application, IntraVUE helps bridge the gap between end-point devices and any user (IT/OT) by using an internet browser to remotely view the status of any piece of equipment with an IP address.

IntraVUE continuously monitors a device's performance and alerts you about potential end-device problems, provides IIoT and Industrie 4.0 aware users with relevant on-demand network-wide site layout diagrams, and generates self-serve uptime performance Analytics reports about the health of your IIoT, and Industrie 4.0 devices to help you restore productivity and uptime.



IntraVUE with its new re-designed user interface in HTML 5 continually scans your entire network(s) for new devices, and immediately updates the user interface and event log information when a device has disconnected, or experiences problems. This dynamic ability is enhanced when IntraVUE Agents are used to visualize remote areas of your IIoT, and Industrie 4.0 infrastructure.

## IntraVUE Benefits

**Popular Industrial Ethernet\IP, Modbus\TCP, Profinet, or WiFi devices that you can Monitor & Manage with IntraVUE™ include:**

Con-trollers	SCADA Devices	IIoT Sens-ors	WiMAX devices	Wearable Devices	PLC Mod-ules	Heat Sensors	Water Well Sensors
RF Radios	Robotic Arms	Inspection Drones	HMI Devices	AR/VR Head-sets	Voltage Sensors	Fleet GPS Vehicle Sensors	Oil & Gas sensors
Smart Grid Sensors	Vibration Sensors	Utilities Sensors	RFID Ware-house Sensors	PoE Cam-eras and Lighting	Traffic Sensors & lights	Alarm & Motion Sensors	Industrial Grade Switches
Zone Enclos-ures Sensors	Fire & Hazard Sensors	Conveyor Belt Sensors	Industrial Access Points (APs)	Autonomous Forklifts	Pallet Hand-ling Sys-tems	Robotic Labeling	Infrared Labeling Readers
Infra-structure & Highwa-y sensors	Solar Panels Systems	Septic and Sewer sensors	Access Control Sensors	Actuators	Mon-itoring Stations	Gen-erators	Energy Con-sumption Sensors

Industrial Pumps	Autonomous Trucks	Fully Robotic Systems	Supply Chain Sensors	Climate Control & Temperature Sensors	Engines and Turbines	Machine-ry Equipment	Any IP device or bridged to IP
------------------	-------------------	-----------------------	----------------------	---------------------------------------	----------------------	----------------------	--------------------------------

**Popular Commercial\Enterprise Ethernet\IP, Modbus\TCP, Profinet, or WiFi devices you can Monitor & Manage with IntraVUE™ include:**

Mobility Devices	Building Automation	IP Surveillance Cameras	Lightning & Room Management	Wearable Devices	Canary Devices	Access Control Devices	Smart Thermostats
Energy Management	POS & Inventory Management	Connected Appliances	HVAC equipment	GPS asset tracking	Door & window locks	Food & Drink Compartments & Dispensers	Smoke & Fire detectors
Coffee Machines	Biometrics Devices	Solar Panels	Connected Lighting Fixtures	Intrusion detection Sensors	Water management	Pollution & Emissions Sensors	Smart Parking Sensors
Digital Signage	Real State management	Gas Station Pumps	Slot Machines	Lift & escalator management	Electrical management	Predictive maintenance	Any IP device or bridged to IP

**IntraVUE™ is good at detecting:**

Duplicate IP and MAC addresses	Intermittent losses caused by noise or vibration	Devices starting to degrade in performance
Accidental loops in cabling	Foreign devices connecting to the	Periodic short bursts of

located in remote electrical enclosures	network (contractor laptops)	broadcast traffic triggered by other devices
Devices accidentally moved to a different port	Cable and connector problems based on crushed, bent, or improperly grounded cable	Redundancy failures using ring or RSTP
Communication lockups or failures (power surges or failures, resets)	Configuration errors	Application Faults (PLC and a SCADA station)
Broken Device Level Ring Networks	Duplex mismatch issues	CRC Errors

### Core Features

KPIs Uptime Dashboard	Automatic IP Network Scanning	Topology Dashboard
Graphical Interactive UI	Threshold graphing	Health Status Logging
Advanced search and filtering options	Real-time tracking of infrastructure changes	Device details via SNMP
24/7 Monitoring and Alerting	Logical Device Location	Device Positioning
Documenting of plant network	Testing of network connections	Testing of full deployments
Filtering View Options	Isolation of Scanned Networks	Multi-Network Scanning
End Device Hyperlinks	New Device Identification	Analytical Reports
Database Export / Import	Bulk Device Properties Export / Import	Support Archives
Email & SMS Alerts	Device Icons	Remote View

Wireless Network Scanning	Centralized Supervisor Dashboard	Multi-Device Dashboard
Isolated Network Scanning	IntraVUE Agent for Isolated Networks	HTML5 Compatibility
Passive Discovery of New Devices	Asset Inventory	Network Changes

**Realize Fast Return-on-Investment:** Once installed, IntraVUE customers typically realize ROI in less than six months, to resolving problems with device connectivity and configuration, and reducing the time and cost associated with network expansions.

**Vendor neutral design:** Supports legacy and modern automation systems and devices from multiple vendors operating on standard, industrial Ethernet while also incorporating industrial Ethernet protocols like EtherNet/IP\* and PROFINET; this provides visibility to the complete plant automation system and helps evolve these systems to modern IoT and Industrie 4.0 architectures.

**Validation tested on automation networks and devices:** Ensures that while providing visibility and analytics, the monitoring traffic will not disrupt live manufacturing or process system activity to increase confidence in system reliability.

**Real-time monitoring:** Pulls relevant and time-critical context and performance details from Ethernet devices within the system, including both networking and field devices, maximizing useful data while minimizing the impact to the network.

**Simplified visualization:** Enables intuitive visibility of the networked automation system within the user interface, with tools to formalized documentation of the Ethernet networked system for improved document control Scalable licensing Offers expansion capabilities as the number of devices at a site grows, and an add-on supervisor highlights visibility of key performance indicators across multiple plants and large networks for future growth.

**Client/server architecture:** Constantly monitors multiple subnet network over local connection while providing convenient visibility and documentation from WAN or VPN client to simplify plant monitoring over long distances.

**Optional hardware appliance for non-routable networks:** Monitors isolated networks without opening them up to the plant network; performs monitoring at the field device and feeds the data to the licensed IntraVUE™ Server to provide holistic visibility to the complete plant network Infrastructure analytics Initiate on-demand analysis of system performance to identify key risks present on the network and determine root cause, improving system uptime and helping move to predictive maintenance of critical infrastructure.

**Key performance indicators:** Provide metrics on performance of critical elements of automation system in 24-hour view and 30-day trending view to increase the uptime and stability of the system.

**Speed Documentation and Deployment:** Available as an Internet download to a laptop or industrial PC, IntraVUE can be deployed quickly and is easy to maintain. As your architecture and number of connected devices increase, IntraVUE can seamlessly scale from a handful of devices to thousands. The software simplifies a variety of deployment tasks, including:

- Support for interactions between the system integrator, installer and the end user
- Validation of as-built versus current state
- Create network topology drawings
- Disaster recovery

**Collect and Document Actionable Data:** IntraVUE documents and stores data in an internal relational database on specific details relating to what is connected to your network, events and time periods providing you with port-by-port mapping. This real-time data delivers a live view of your network as well as details for diagnostics and advanced analytics.

- Continuously scans connected devices
- Identifies and tracks changes

- Does not need to be connected (providing offline views)
- Does not require seat licenses (downloads are free)
- Can run on numerous computers in distributed architecture

**Diagnose Network Problems from Any Location:** Designed for immediate problem analysis or periodic maintenance reviews, IntraVUE online Diagnostic Report Generator is accessible 24/7/365 from any laptop, tablet or smartphone—on-site or remotely. Users can generate various reports, which are targeted to the skills and responsibilities of that user. Once requested, reports are available via email in minutes. From the diagnostic report, the user can work with IntraVUE data analysis tools including event logs and trend reporting to definitively identify root cause and establish resolution to the problem.

**Use Advanced Analytics to Accelerate Troubleshooting:** IntraVUE narrows the scope of problem detection by establishing key performance indicators (KPIs) and generating daily KPIs reports that provide instant access to information on issues affecting critical equipment.

**Anywhere Access:** Diagnostic and KPIs Reports are available 24/7/365 via laptop, tablet or smartphone on both iOS and Android devices. Report details are tailored to the responsibilities and skill levels of various users, including:

- Maintenance technicians
- Control engineers
- Manufacturing IT and network professionals

**Pinpoint and Resolve Connectivity Failures:** Once the most critical areas of concern have been identified either by the on-demand Network Analytics report or by visual representation of the IntraVUE interface, you can return to IntraVUE to access granular views, by device. Drill-down boxes provide information at the device level about:

- Connections
- Event histories

- Support documentation

In addition to the software, Panduit also can provide IntraVUE users with advanced features and hardware that:

- Enables users to have visibility to non-routable networks and islands of automation
- Can be installed at multiple sites
- Access dashboards with trend graphing
- Automatically assign static IP addresses to edge devices

Simplify the Management of Ethernet Connectivity With fast, simplified problem detection and diagnosis, IntraVUE enables manufacturers to gain a reliable, secure, robust physical layer network in today's complex and highly sensitive industrial automation ecosystem.

Next: [Installation & Registration](#)

## Installation & Registration

### What do I need to know before installing IntraVUE™?

IntraVUE Readiness Checklist

Follow these 9 steps to install IntraVUE and quickly Discover, Map, Monitor and Diagnose the health of your industrial plant network.

#### Step 1:

Request a demo or official license to run either the POC, Assessment, or IntraVUE installation from [techsupport@panduit.com](mailto:techsupport@panduit.com).

#### Step 2:

Designate which Windows workstation, server, virtual, appliance, Raspberry Pi, etc., will be utilized. Refer to the [System Requirements](#).

#### Step 3:

---



Define the preferred scanning location. The ideal place is where IntraVUE can successfully ping all edge devices (e.g. the core switch). Refer to [IntraVUE Placement](#).

### Step 4:

Assure SNMP is enabled in all fully managed switches. Know the read only community that can be configured in IntraVUE if it is not the default of 'public'. See [System Requirements](#) on what is considered a fully managed switch.

This is not mandatory. You can still monitor edge devices and view the network topology with some manual work.

### Step 5:

Identify the IP scan ranges of all devices.

### Step 6:

Install and register the latest version of IntraVUE. Refer to IntraVUE [Installation & Registration](#).

### Step 7:

If Access Control Lists (ACLs) or management lists are configured in managed switches, make sure the IP of the IntraVUE host is configured to allow access. Refer to the IntraVUE [System Requirements](#) to open access for the communication ports.

### Step 8:

Select the first network and start scanning. Make sure there are no devices that stay in 'Unresolved' and that devices move under the managed switches. If switches are in a different network, they must be included in the scan range of the network chosen. Once the first scan is complete, continue by adding the remaining networks. Refer to [Completing Initial Configuration](#).

### Step 9:

Create your Plant Documentation. Refer to [Creating Plant Documentation](#)

This check list can also be downloaded [here](#)

---

IntraVUE System Requirements

---

The IntraVUE™ system and configuration requirements are shown below. Because IntraVUE is used in industrial automation environments, the next requirements are meant to make running IntraVUE easy.

### Host System Requirements

Server	
<b>Processor</b>	Dual Core with Cache (minimum), Quad Core with Cache (preferred), however, IntraVUE has been designed to work with any modern low power processor. Hyper-Threading recommended only when IntraVUE is installed on a virtual machine.
<b>RAM (available)</b>	2 GB: Up to 500 nodes, 4 GB: 500+ nodes, 6 GB: 1000+ nodes, 8 GB: 1500+ nodes
<b>Free Disk space</b>	4 GB: Up to 500 nodes, 6 GB: 500+ nodes, 8 GB: 1000+ nodes, 12 GB 1500+ nodes
<b>OS</b>	<p>Workstations OS: Windows 7 32-bit and 64-bit, and Windows 10. Server OS: Windows Server 2008, 2012, and Server 2016.</p> <p><b>Vista, and Windows 8 (and variants) are not certified nor recommended.</b></p> <p>Linux: Only available on a pre-configured VMWare Virtual Machine image. Click <a href="#">here</a> for more information.</p> <p>When installing on Windows 7 ALWAYS choose a folder outside Program Files to avoid read-only file permission problems. We recommend a folder such as C:\IntraVUE.</p> <p>If you install on a Server based system, you MUST use the Add Programs function of Control Panel's Add/Remove Programs.</p>

<b>Virtualization</b>	Any hypervisor platform that supports the operating systems above and that has a fixed virtual machine ID (VMID) not susceptible to high-availability changes is required.
<b>Required Software</b>	<p>(Java JRE will be automatically installed as part of the IntraVUE™ installation). User interfaces does not make use of java. Only used for the scanning engine.</p> <p><b>Java 6 should be uninstalled to avoid unexpected behavior of IntraVUE™.</b></p> <p>The latest Java JRE 32-bit at the time of the build will be installed as part of IntraVUE™ Installation. In 64-bit windows computers, only the 32-bit version of the Java Runtime Environment (JRE) should be installed (i.e. under C:\Program Files(x86)\Java).</p>
<b>Antivirus / Anti-Malware</b>	Antivirus software must be disabled/turned off during the installation. You can turn them back on when the installation completes. You may have to configure your AV exclusions to skip the C:\intravue folder in order to allow the IntraVUE™ installer to complete installation.
<b>Database</b>	<p>(Maria DB will be automatically installed as part of IntraVUE™ Server Installation and removed as part of the IntraVUE™ uninstaller).</p> <p>*The C:\MySQL folder must be excluded from being backed up or analyzed by virus checking programs. The programs will lock critical, large files and cause the mysql service to stop if it cannot access certain files for longer than a few seconds. Should this occur, restarting the msyql service always works, but there will be no IntraVUE data collected while mysql is stopped.</p>
<b>Web Server</b>	(eTomcat will be installed as part of IntraVUE™ Server

---

	Installation). This is used by the user interface.
<b>Client</b>	
<b>Web Client</b>	Any browser that supports HTML 5 and JavaScript is required. Recommended browsers include Chrome (most recent), Firefox (most recent), and Internet Explorer 11 (or most recent).
<b>Mobile</b>	
<b>Mobile Client</b>	Android smart phones and tablets 5.0 (or newer versions recommended). iPhone devices will be supported in the future.

### IntraVUE Scanning Requirements

SNMP Requirements in detail	
<b>Fully Managed Switches:</b>	These switches must conform to the minimum SNMP standard RFC 1493 (or one of its successors) and respond to the Bridge MIB, or the Q-BRIDGE-MIB (RFC 2674 or one of its successors) in the case of newer Fiber Switches. See <a href="#">Verifying SNMP on Fully Managed Switches</a> before attempting to buy switches that advertise as such but do not confirm with these SNMP standards.
<b>SNMP Support:</b>	SNMP must be enabled on all Fully Managed Switches
<b>SNMP Community</b>	Fully managed switches must have at least one Read-Only community (e.g. public) available
<b>Local access to devices:</b>	The host server must be able to PING all the devices in the scan range
<b>Layer 3 Routing:</b>	Gateway address required when monitoring remote subnets or VLANs

<b>Access Control Lists:</b>	May need configuration to allow scanning using required ports (See below)
<b>Firewalls / Intrusion Systems:</b>	May need configuration to allow scanning using required ports and protocols
<b>HTTP Access</b>	Required to allow remote access to user interface and devices web servers (See ports below)
<b>Network Bandwidth:</b>	The switches must provide timely responses to SNMP queries. Typical response times are less than 20 milliseconds but some switches are known to take 20 seconds (20000 milliseconds). IntraVUE will tolerate a response as slow as 1000 milliseconds (1 second).

### Ports used by IntraVUE

#### Required Ports

**80** (TCP) – used to find devices with web pages and to provide a link to those pages automatically. May also be used as additional port to browse to IntraVUE if it does not conflict with IIS.

**8765** (TCP) – mandatory port to browse IntraVUE™ using HTTP

**OR**

**8766** (TCP) - mandatory port to browse IntraVUE™ when using HTTPS

**161** (UDP) – used for SNMP communication with managed switches

**162** (UDP) – used to listen for SNMP trap messages

**137** (UDP) – used to find NetBIOS names

**44818** (UDP) – used for Ethernet/IP CIP protocol

#### Optional Ports

**65402** (UDP) – used for communication to IntraVUE Agents

---

**65403** (UDP) – used for communication to IntraVUE Agents

### Testing Local Access to Devices

The IntraVUE™ Server must be able to PING all the devices in the scan range. Open a dos command prompt and type "ping x.x.x.x" replacing x.x.x.x with the ip address of a device in the scan range. If the ping command returns "Reply from ..." without timing out then the device passed this requirement.



If any device is in a different subnet, you should be able to PING them using the TRACERT dos command (e.g. c:\> tracert "192.168.0.1." or similar) which will yield the last hop router leading to the device. The IP address previous to the target device in the output results is the gateway address required as top parent in the next section.

Layer 2/3 switches store the mac addresses of connected devices in the scan ranges and must be configured to respond to SNMP from the IntraVUE host. This requires that an SNMP Read-Only Community be configured on these devices and may require additional permissions such as an entry in an Access Control List (if applicable).



IntraVUE will not be able to map the full topology if SNMP is not enabled and SNMP Read-Only Communities are not configured on all L2/L3 switches in the plant floor. Install IntraVUE and use the switchprobe utility to confirm this requirement before proceeding. See [Verifying SNMP on Fully Managed Switches](#).



When enabling SNMP and SNMP Read-Only Communities on some L2/L3 switches you may be required to perform a reboot to allow changes to take effect.

The switches must provide timely responses to SNMP queries. Typical response times are less than 20 milliseconds but some switches are known to take 20 seconds (20000 millisends).

IntraVUE will tolerate a response as slow as 1000 milliseconds (1 second).



See also [IntraVUE Architecture](#)

### IntraVUE Placement and Scanning Scenarios

The following are the most common physical network configurations where IntraVUE is used or can be used to scan the "local area network" (i.e. all devices that are exclusively inside a plant site without having to go through the WAN or IT networks). It's important to know which one if you type of network so that you can place IntraVUE accordingly.



1

2

It's important to scan locally your plant network as many **CIs** are being connected to **IT** networks using TCP/IP equipment that could create a backdoor of weak points from vulnerable IT systems where **APT**<sup>3</sup> attacks could bring down automation systems.

### Deployment Options:

- » Deploy IntraVUE™ as an application on a Windows Server or Windows PC (most Common)

### IntraVUE Placement Options:

IntraVUE should be placed local to the end devices it is expected to monitor and then users can browse from remote locations to see what is happening

---

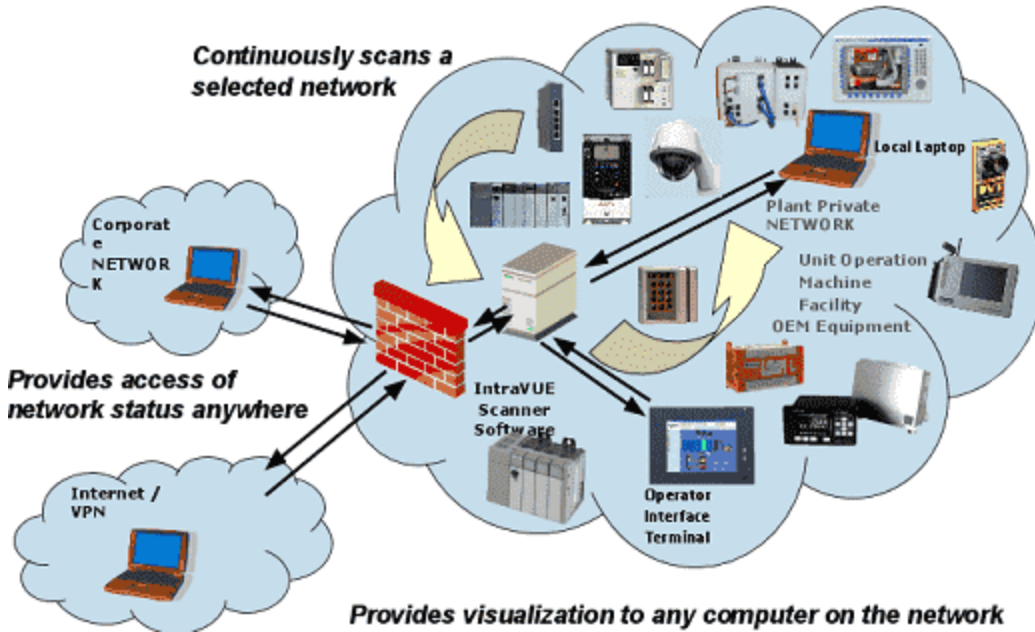
---

<sup>1</sup>Critical Infrastructure (e.g. SCADA, TCP/IP)

<sup>2</sup>Information Technology. Corporate group that manages the core network but not necessarily the automation networks.

<sup>3</sup>Advanced Persistent Threat: a group of hackers that develop hacking tools that uses multiple attack vectors for long undetected periods of time in order to compromise and control a target plant network. These tools can by-pass firewalls, IDS, and even Anti-Virus software.

---

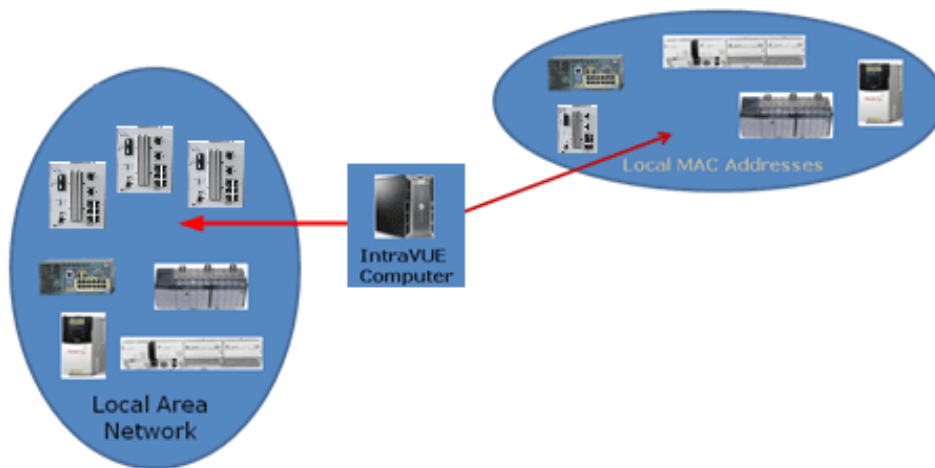


The IntraVUE™ host should be inside the same subnet as the edge devices for best results without a firewall in-between. The IntraVUE host should always be connected to a (layer 2) managed switch to obtain SNMP data!

## Scanning Scenarios

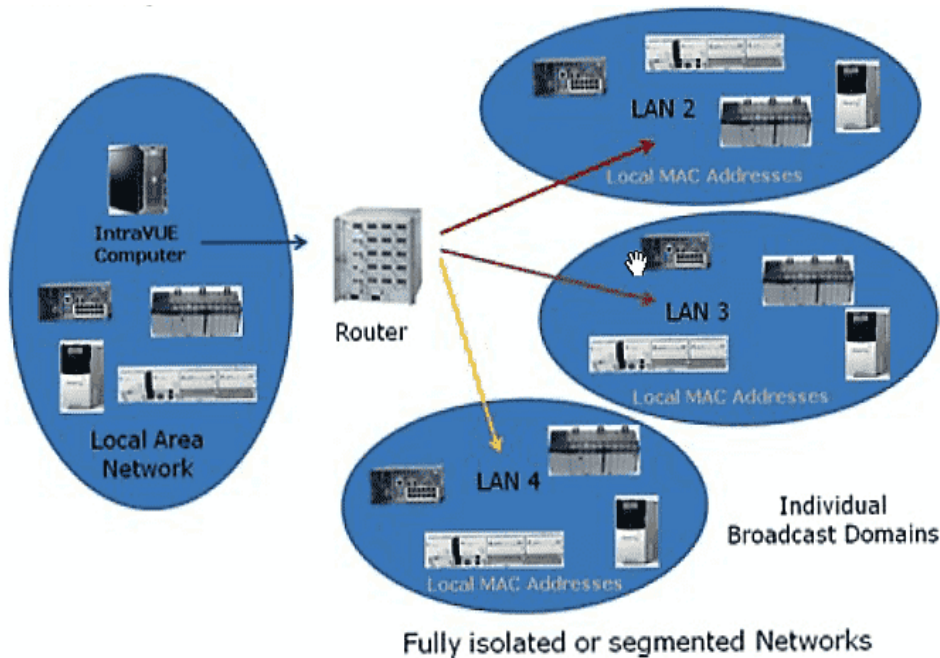
**Simple Network:** The simplest network in which all the edge devices and all the switches are in the same subnet (e.g. scan range 192.168.0.1 - 192.168.0.254). To scan this type network you only have to enter the full scan range and proper SNMP communities. If this is your network, you do not have to read the rest of this document. IntraVUE was designed for this type network when the subnet mask is 255.255.255.0 (Class C) and there is not router required. Each 'cloud' represents different 'physical' plant zones, but all devices are pingable from the Top parent which is the IntraVUE host.



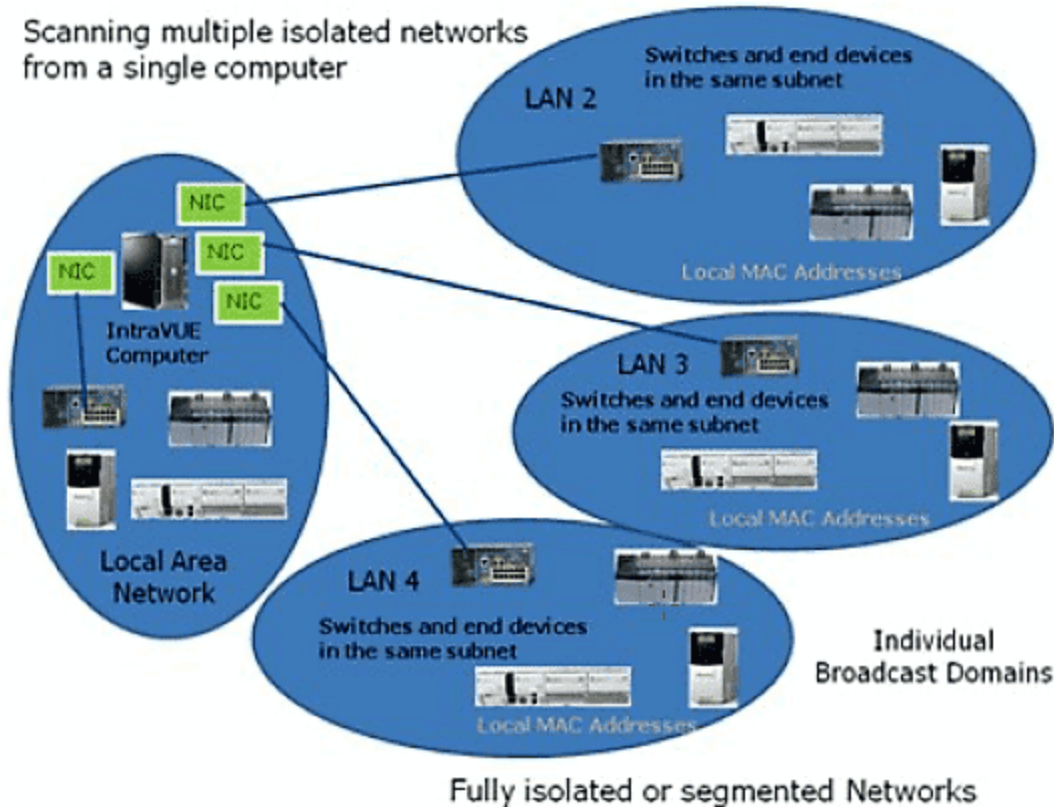


**Multiple LANs from a single IntraVUE host using a router in between.** Another simple network is one in which all the edge devices are in one subnet and all the infrastructure switches are in another subnet. The IntraVUE Server should be in the subnet of the edge devices and should be the top parent of the IntraVUE network. The IntraVUE Server is on the left scanning all the LOCAL edge devices communicate without going thru a router. However, the IntraVUE Server must go through a router in order to get ping and SNMP data from the switches to the remote networks. The router (which knows the macs of the switches) must be in the scan range of the same IntraVUE network and respond to the same SNMP read-only community configured in IntraVUE. See [Configure Menu - Scanner Tab](#).

---



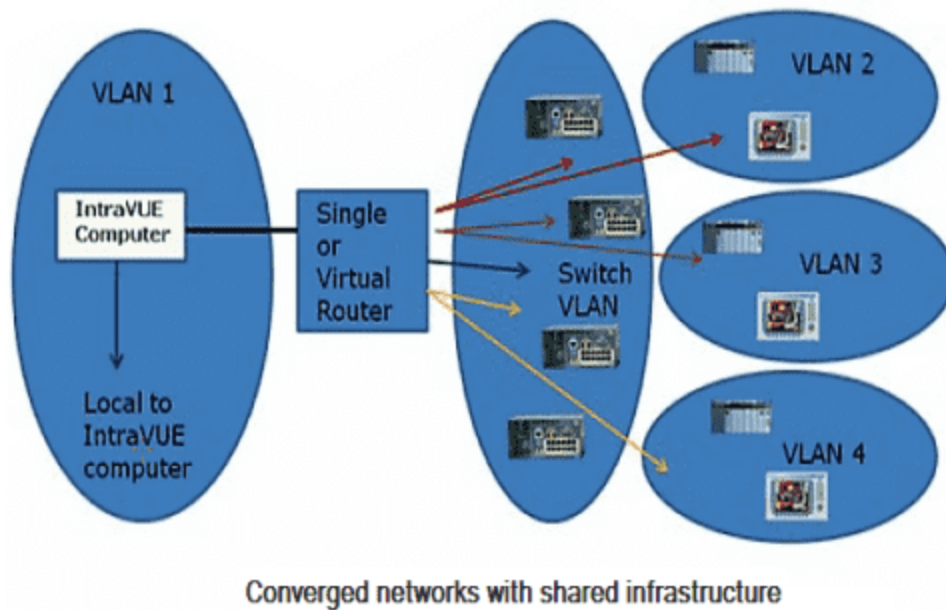
**Multiple NIC cards and No Router or SNMP:** In some cases, plant personnel are not allowed to know the SNMP community of the central router or access switch. In the next figure, a NIC card has been added for each formerly remote LAN to solve this problem. Now those LANs have local addresses on the host computer and communication does NOT go through the router. The MAC addresses of all devices are in the host computer local ARP cache. This configuration is also useful when IT departments isolate private LANs using VLANs or a firewall and SNMP is not allowed to go through. The use of Virtual Machines where the IntraVUE agent can be installed to scan those private LANs or VLANs solves this problem. However, if the number of virtual machines using IntraVUE agents is over whelming or costly to manage, we recommend instead using IntraVUE appliances installed as agents within those private LANs or VLANs. See [Using the IntraVUE Appliance as an Agent](#) and [IntraVUE Appliance Configuration](#) for more details.



**Networks using VLANs:** is made more complex by configuring the layer 2 switches in the network to have VLANs. This is one of the most common plant floor network architectures. There are 5 VLANs. The layer 2 switches are in the center circle, Switch VLAN. Even though they are connected by layer 2 switches, devices in one VLAN can not communicate with devices in another VLAN without going through the router. For IntraVUE to provide the most diagnostics, each VLAN of edge devices should be a separate IntraVUE network in the System Configuration Scanner Tab. Each one of the 'remote' networks must also include the interface (Gateway IP address) of the router leading to the edge devices (as determined by DOS command TRACERT) as the top parent. In the next figure, the IntraVUE network for VLAN 1 needs to have the local computer as top parent, all the local IP addresses, the router, and the switch IP Addresses. VLANs 2, 3, and 4 each need to have the IP address of the router as top parent, the IP addresses of the VLAN, the router, and switch's IP addresses all in the scan ranges of that IntraVUE network. (The switch's IP addresses will be in all 4 IntraVUE networks.) VLANs are configured in a layer 2 switch by assigning VLAN numbers to ports of the switch. Packets arriving on a port of a switch having a VLAN(s)

---

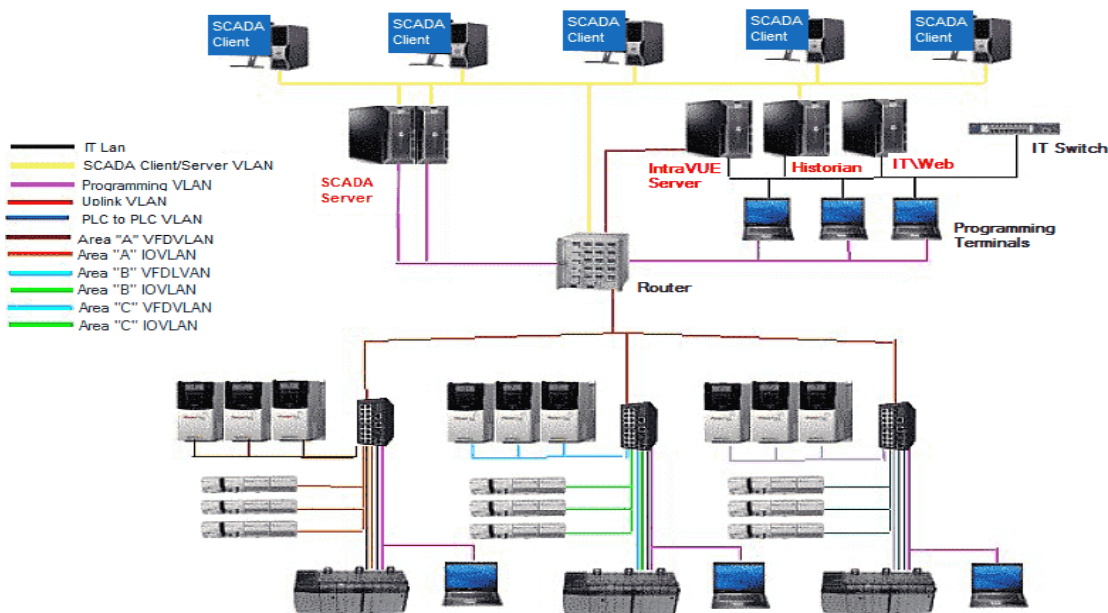
configured will only be sent to other ports having the same VLANs configured. This limits broadcast traffic to only the ports with the same VLAN number as the originator.



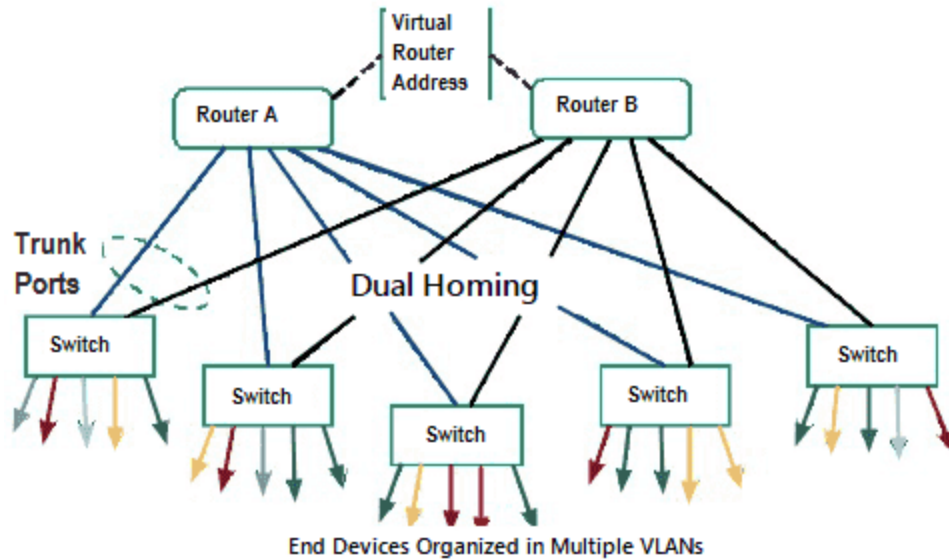
**Multiple VLANs:** using different colored lines for each VLAN. If the destination MAC is on a port in another VLAN, the message will be sent to the gateway and then back to the switch on the port having the same VLAN number as the destination. If a port of a switch is not configured for a VLAN, it acts as if all VLANs are configured for that port. All traffic for a device in a different VLAN (different colored line) must go to the router to be redirected to the switch.

Implementing Rapid Spanning Tree protocol (RSTP) in the switches creates a physical ring of communication where the last switch in a series of connected switches is connected to the first switch, thus forming a ring. The last link is never 'active' unless there is a break between any other switches in the ring. At that time, communication will start a new path and all switches will continue to be able to communicate, but using a different path. Nothing special needs to be done to handle this situation. IntraVUE will discover the new path and redraw the topology to reflect the change in the ring.

## Multiple VLAN Architectures



**Hot Standby Redundant protocol: (HSRP)** creates a connection between a pair of routers. In this scenario 2 routers are configured so that either one can act for the other in the event the other router fails. The routers 'share' a virtual IP address and a virtual mac address as well as having their own ip and mac. In some cases, one router will respond to the virtual IP/MAC Address, but the other can assume in within milliseconds if necessary. In many cases, each router handles some VLANs. Router A will handle the even VLANs and router B will handle the odd VLANs. Other devices are configured to use the 'virtual' IP address of the routers. Additionally each 'upper level' layer 2 switch is connected to both routers, so that if a router failure happens there is a connection to the other router using the same 'virtual' IP address. Since the routers are connected and the upper switches are connected to each router, an alternate path is created and the mac of the routers can be seen on two possible ports of the 'upper level' switches.



## Isolated Networks behind a Gateway, PLC, Private VLANs, Firewalls, NATs

### The IntraVUE Agent



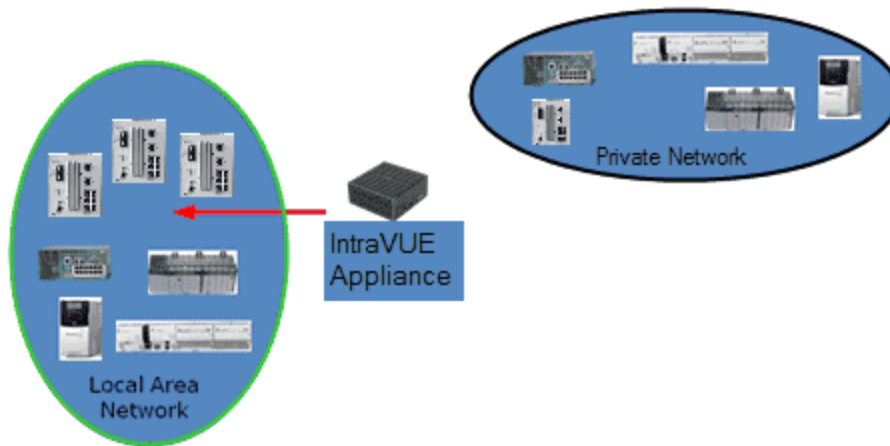
The IntraVUE Appliance is a small-factor headless appliance strategically placed in a network closet at a remote site with the purpose of scanning edge devices in one or multiple cases below:

1. Devices in an isolated network behind a gateway. A switch inside the 'isolated network' behind a gateway using one port of the agent and the other port of the agent is connected to a switch on the 'plant' side (or plant VLAN Access) network.
2. Private VLANs. One is the private VLAN of the 'system' and the other provides access from the 'plant' to the PLC of the 'system'. The IntraVUE Agent has one interface connected to a 'system VLAN' port of the switch and the other agent's Ethernet interface is connected to a 'plant VLAN' port of the same switch.

3. If a NAT, or Firewall Access to the NAT, or Firewall devices is configured to send all packets from an IP address on the plant side to the IP of the IntraVUE agent on the 'system' side of the NAT/Firewall, then the IntraVUE Agent can scan the devices behind the NAT, or Firewall.

### Using IntraVUE Appliance as an Stand-alone Server to scan the Plant Network:

When there is no physical server or virtual machine available, the small-factor headless appliance can be deployed as an IntraVUE Server. The only differences is that it does require software registration and only one port of the appliance is connected to a switch on the 'plant' side.



See [Using the IntraVUE Appliance as an Agent](#) and [IntraVUE Appliance Configuration](#) for more details

---

## Install / Upgrade and Register IntraVUE™ 3

IntraVUE Installation or Upgrade Instructions

Installation or Upgrade Instructions of IntraVUE™ full version for Windows Based Systems

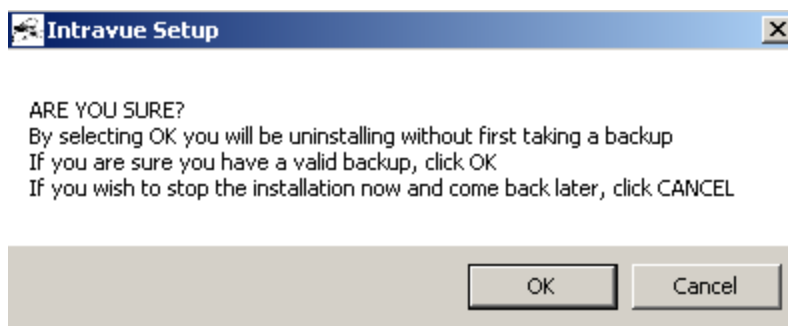
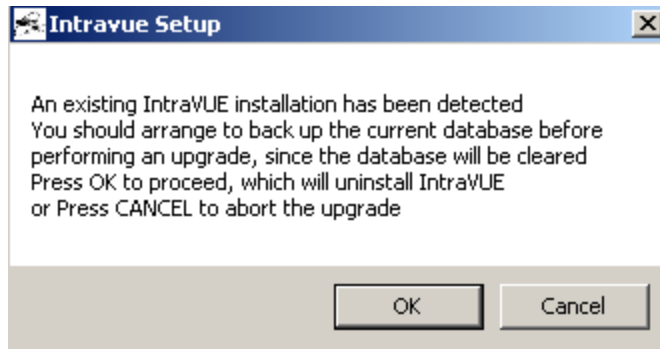


Before you install or Upgrade IntraVUE you will need to have an active support contract or active IntraVUE subscription before you can register your Product Key (PK). The

---

IntraVUE Web registration portal will reject your PK if you do not have either requirement. You will need to contact a distributor near you to renew either one.

1. Download the latest Intravue\_.x.x.exe installer. See Downloads
2. Right-Click Click Intravue\_.x.x.exe and select "Run as Admin"
3. Click "Next" for on the Welcome to the IntraVUE Setup Wizard screen
4. Click "I Agree" to the License Agreement.
5. Select "Install" for Choose Install Location. Default location is set to C:\intravue but you can change.
  1. If you're upgrading, you will receive a notice to make a backup of your current database. Click "OK" to continue with the upgrade.
  2. IntraVUE will make a backup of the appropriate folders and store them automatically in "prevxxxx" folders under C:\intravue when you run an upgrade.

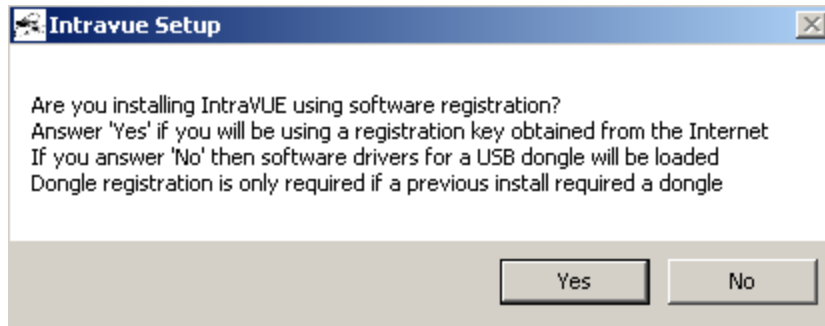


6. Select "Yes" to use IntraVUE™ with a software license key. If you purchased an IntraVUE USB dongle select "No".





This question is used to determine where IntraVUE should look for licensing information (c:\intravue or from a USB dongle)



7. A Java Setup - Welcome window appears whenever java is not installed in the machine. Click "Install" and let the Java Install run its course.



Java 32-bit will be installed as part of the installation. If the version of Java is out-dated Java prompt you to remove Out-of-Date version. The UI does not make use of Java 32-bit, but it's only used the for the scanning engine.

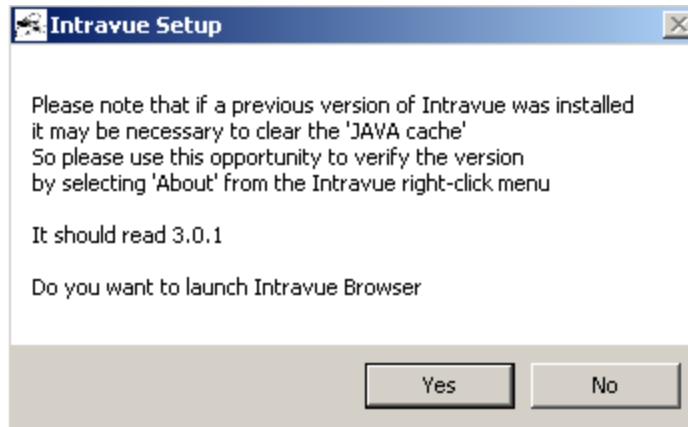
1. Click "Next" at the "Restore Java security prompt" when asked.
2. Click "Close" to finish the Java installation



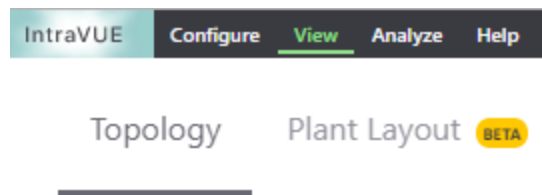
JAVA might prompt you to update. Ignore as IntraVUE™ will install a 32-bit version of Java

8. Close the "Verify Java Version" Internet Browser.
-

9. Click “Yes” to “Do you want to launch IntraVUE™ Browser”



10. Once the browser window launches, if you get IntraVUE™ logo at the top your installation performed successfully.



11. You can Open IntraVUE™ in any compatible browser such as IE 11, Chrome or Firefox. See for details.



Pay close attention to the following issues that might prevent you from opening up using IntraVUE™ correctly.

- » Ensure the IntraVUE 3 URL (<http://127.0.0.1:8765/iv3/>) is showing in the URL address bar and is in trusted sites on the security tab of IE's Tools > Internet Options (uncheck 'only use https'). This helps pop-up dialogs appear.
- » If you are being redirected to the old URL <http://127.0.0.1:8765/iv2/ivue.jsp> in Internet Explorer you either have an IE version earlier than v11 or you need to reset your browser settings from >Tools > Options > Advanced > Reset Internet Settings and reboot.
- » In the Windows services (Start > Run > `services.msc`) make sure the services are running: 'Apache Tomcat etomcat', 'Auto-Ip Server', 'Autoip Ping Daemon', 'Mysql'.

- » If you get a white/blank screen when you browse to IntraVUE in Internet Explorer, remove 127.0.0.1 (or IntraVUE host's ip address) from the websites listed under Tools > Compatibility View Settings > "Websites you've added to Compatibility View".
- » It is required to install the included 32-bit Java JRE included with the IntraVUE software install since the IntraVUE Scanner does not support running on 64-bit Java JRE.
- » We recommend you set Java to NEVER update. IntraVUE software does not support 64-bit Java.
- » Microsoft Windows update could stop some services from fully starting.  
The IntraVUE services will try to restart themselves for about 3 minutes but the Microsoft messages such as "please do not turn off the computer while updates are applied" stop some of the IntraVUE services from starting. In the Windows services (Start > Run > services.msc) start these services if they are not running: 'apache tomcat etomcat', 'autoip ping daemon', 'mysql'.



See [New Installation](#) for more installation details

---

### Registering IntraVUE™ 3 Product Key or Dongle

#### Registration or Upgrade of IntraVUE™ Product Key



If you are registering or updating an IntraVUE dongle proceed to 'Register IntraVUE when using a dongle' down below.

1. Invoke IntraVUE™ from your desktop or open an internet browser and enter `http://127.0.0.1:8765` in the address bar if IntraVUE is installed on the same computer, otherwise change 127.0.0.1 to the IP address or URL of the IntraVUE host. Press Enter.
  2. Click > Configure > Login as user "admin" > password "*intravue*".
  3. The Registration link will immediately appear.
-

4. Copy the KEYCODE number. You'll need this number in the next step.
5. Obtain an IntraVUE registration code from the IntraVUE User Web-Based Registration by clicking "here" next to "To get a registration code" or entering this address into a second tab <https://intravuerereg.panduit.com/intravue-registration/index.php>
6. Within the web registration form, Enter your Email Address, Organization, KEY CODE, PRODUCT KEY and SERVICE CODE (As Provided by Panduit with your purchase). Click "Submit Query".

#### IntraVUE User Web-Based Registration V2.6 7/21/2015

user name (email please):	<input type="text"/>
user organization:	<input type="text"/>
Product Key (25 chars):	<input type="text" value="From Purchase Order"/>
Key code (case sensitive - usually upper case):	<input type="text" value="Same as in IntraVUE Registration"/>
Registration Code (to set in Intravue):	<input type="text" value="press 'Submit' to obtain registration"/>
Service Contract Code (to set in Intravue):	<input type="text" value="From Purchase Order"/>
	<input type="button" value="Submit"/>

When all fields are filled and you press 'Submit' you get a registration code FFFF...

Please use a valid email address because then it will be possible for us to advise you of any updates to the IntraVUE product

7. Copy the returned "Registration Code" (e.g. FFFF...) into the Registration Code field in the IntraVUE's "REGISTRATION" page. This activates IntraVUE™ to enable monitoring of Automation Networks.
8. Copy the "Product Key" into the "PRODUCT KEY" field in IntraVUE's "REGISTRATION" page. This activates the IntraVUE product itself.
9. Copy the "Service Contract Code" into the "SERVICE CODE" field in the IntraVUE's REGISTRATION page. This activates the KPIs system and other add-on features of IntraVUE™ provided for customers under Support. If target software is not currently under support, the "Service Contract Code" field will remain blank.
10. Click 'Submit Registration'. At the top of the REGISTRATION page should show something "Your registration has been completed successfully". If it does not call Tech Support.

## REGISTRATION

Your registration has been completed successfully.



Your Product Key might be rejected by the web registration system for several reasons. See this knowledge base article for more details: [KB4473](#)

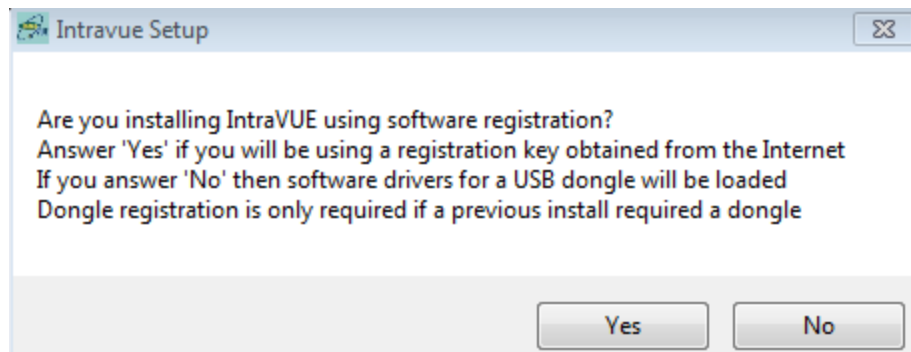


Make sure there are not trailing blank spaces as this will prevent the IntraVUE™ User Web-Based Registration from completing your request successfully.

Register IntraVUE when using a dongle

Register & Upgrade IntraVUE™ by entering license information (dongle-only)

1. If you selected 'No' (for using a USB dongle) during the initial IntraVUE installation, plug the IntraVUE Dongle into the machine now.



Dongles are shipped without registration. They are registered the same way as Software Product Keys. The Dongle will show up having a key code starting with 999xxxxxx. If you do not see that, then the dongle is not recognized. You may have answered Yes to # 1 above. Try re-running the install and answer 'No'. If the problem persists contact Tech Support.

2. Follow steps 1-10 from above (i.e. Registration & Renewal non-dongle)
  3. Message "Invalid Service Contract code" will change to
-

---

## REGISTRATION

Your registration has been completed successfully.

Refer to the dongle steps for an alternate dongle registration & update process

---

### Completing Initial Configuration

## IntraVUE Analytics

The IntraVUE 'Analytics' currently defined in the KPIs system and the Diagnostic Report Generator are intended to supplement or substitute for the need for continuous monitoring or frequent event escalation. If a controls engineer can learn to recognize the health of his network by submitting a database archive to the Analytics Reports generator to allow for subtleties to be identified, then less time is spent diagnosing and more time is spent repairing. By plant managers looking at a summary KPIs display and learn the value of visual management that IntraVUE™ provides, they improve the plant OEE rating.

Start by identifying what devices should be monitored for KPIs in [Completing Initial Configuration](#)

If you already know what devices to analyze KPIs follow the next steps:

Setting Critical States

Critical States are set to one of the 4 critical values in .

CRITICAL STATUS

Intermittent	▼
Unknown	
Ignore	
Intermittent	
Always On	

- » Unknown - devices which have not been configured.



Standard KPIs and Supervisor KPIs Analytics do not take metrics from devices with "Unknown" critical status.

- » Ignore - a conscious decision was made that the device is not critical and statistics for this device should not be in the KPIs reports.
- » Critical Intermittent - A critical device which may not be connected 100% and uptime should not be reported. All incidents are reported.
- » Critical Always On - A critical device expected to be on 100% of the time for which uptime and incidents are reported.

You can set Critical States on a device by device basis from the [Side View in Edit Mode](#) or you may do it in bulk using the [Export / Import](#) mechanism. If using the import / export method, be sure to set at least one device to a critical state or you will not see the correct column, "PKI.critical", in the csv export.

Critical Values for this column in the .csv export are:

- 0: Unknown
- 1: Ignore
- 2: Critical Intermittent
- 3: Always On

---

### Device List View

The Device List view is a report view that lets you see network information related to all devices visible in either the Topology or Plant Layout views.

- » IP Address: The IP of the Device
  - » Network Name: The IntraVUE network the device is configured with (See [Configure Menu - Scanner Tab](#))
  - » Device Name: From CIP or Netbios. Can be modified here (See below).
-

- » Critical Status: See [Device Configure - General](#) & [IntraVUE Analytics](#). Can be modified here (See below).
- » Admin Verified: See [Admin Verification in IntraVUE 3](#). Can be modified here (See below).
- » Type: Device or Switch. Can be modified here (See below).
- » Revision: e.g. ENETIP Rev 7.01. Can be modified here (See below).
- » Vendor: e.g. Rockwell. Can be modified here (See below).
- » Model: e.g. 1756-EN2TR. Can be modified here (See below).
- » Location: e.g. Electrical Room
- » User Defined 1. Custom field. See [Device Configure - Other Names](#)

IntraVUE Configure View Analyze Help							
Topology Plant Layout <span>811A</span> Device List Filters Event Log Diagnostics							
Type to filter data...							
IP Address	MAC Address	Network Name	Device Name	Critical Status	Admin Verified	Type	Revision
<a href="#">10.132.56.83</a>	00:50:56:b4:8a:2e	56	PLN-INTRAVIEW83	Always On	Yes	Device	--
<a href="#">10.132.56.1</a>	00:23:33:6e:31:3f	56	PLN-SSRG-4510-1X-A.panduitlabs.com	Always On	Yes	Switch	--
<a href="#">10.132.56.11</a>	00:07:6e:02:4e:58	56	no name	Always On	Yes	Device	--
<a href="#">n/a_694</a>		56	n/a_694	Unknown	No	Device	n/a
<a href="#">10.132.56.234</a>	00:0f:9c:05:45:87	56	PLN-SSRG-PVIQ-1X-1E-01	Always On	Yes	Device	--
<a href="#">10.132.56.229</a>	00:0f:9c:05:45:a9	56	PLN-SSRG-PVIQ-1X-1A-01	Always On	Yes	Device	--
<a href="#">10.132.56.236</a>	00:0f:9c:05:45:82	56	PLN-SSRG-PVIQ-1X-3-01	Always On	Yes	Device	--
<a href="#">n/a_1340</a>		56	n/a_1340	Unknown	No	Device	n/a



Selecting the IP address of a device will center that device in the Topology View.

### Modify a Field directly from Device List View:

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Log in from the right-top corner using the default password "intravue".
3. By clicking on "Device List", you will see a list of all devices found.



4. Change the either Device Name or Critical Status by clicking double clicking on the actual value for that device until you notice that the value becomes editable. Most values are editable
  5. When done click on an empty area away from the field until you get a blue "Save Changes" button. Click on it to save changes and move to the next row. Continue doing this for devices that need changes.
- 

### Analyze

The Analyze view provides KPI reports when devices are configured for KPI. There are 3 KPI Reports - Daily KPI, 30 Day KPI, and KPI By Networks. These are available from the Analyze button on the navigation menu.

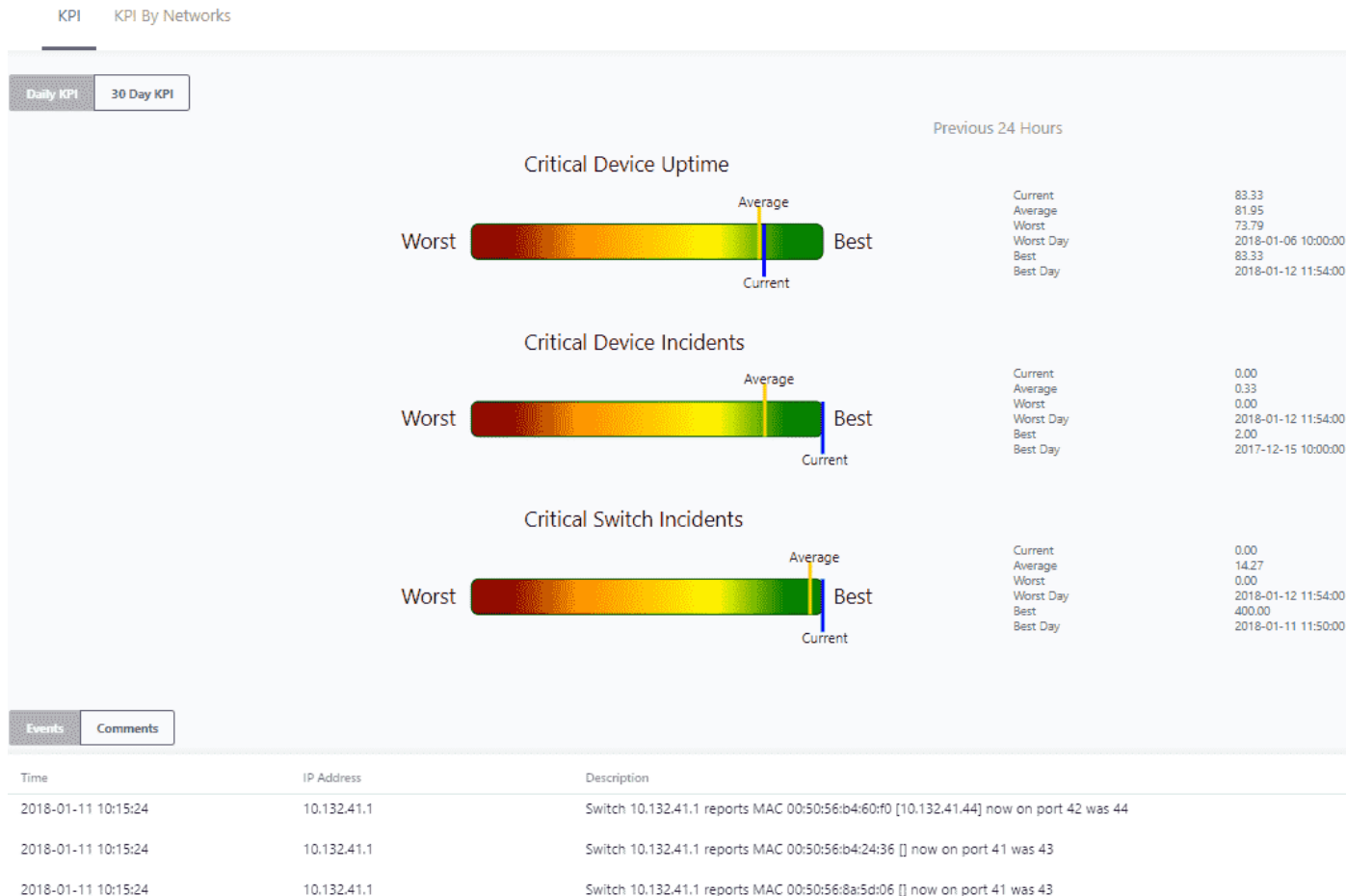
### Daily KPIs

The Daily KPIs report is designed to show you how conditions in the last 24 hours compare to the conditions for the same devices over the last 30 days. It can be accessed by clicking the 'Analyze' button in the latest version.

The three bar graphs with the left side representing rainbow bars show the worst value in the last 24 hours, and the right side representing the best value for the last 24 hours.

There are two vertical bars extending below and above each graph. The yellow bar indicates the daily average for the last 30 days and the blue bar indicates the current day's position between the 30 day best and worst conditions.

---



The Daily Report tells you how today compares with the past. It is a quick indication if things are getting better or worse in the plant.

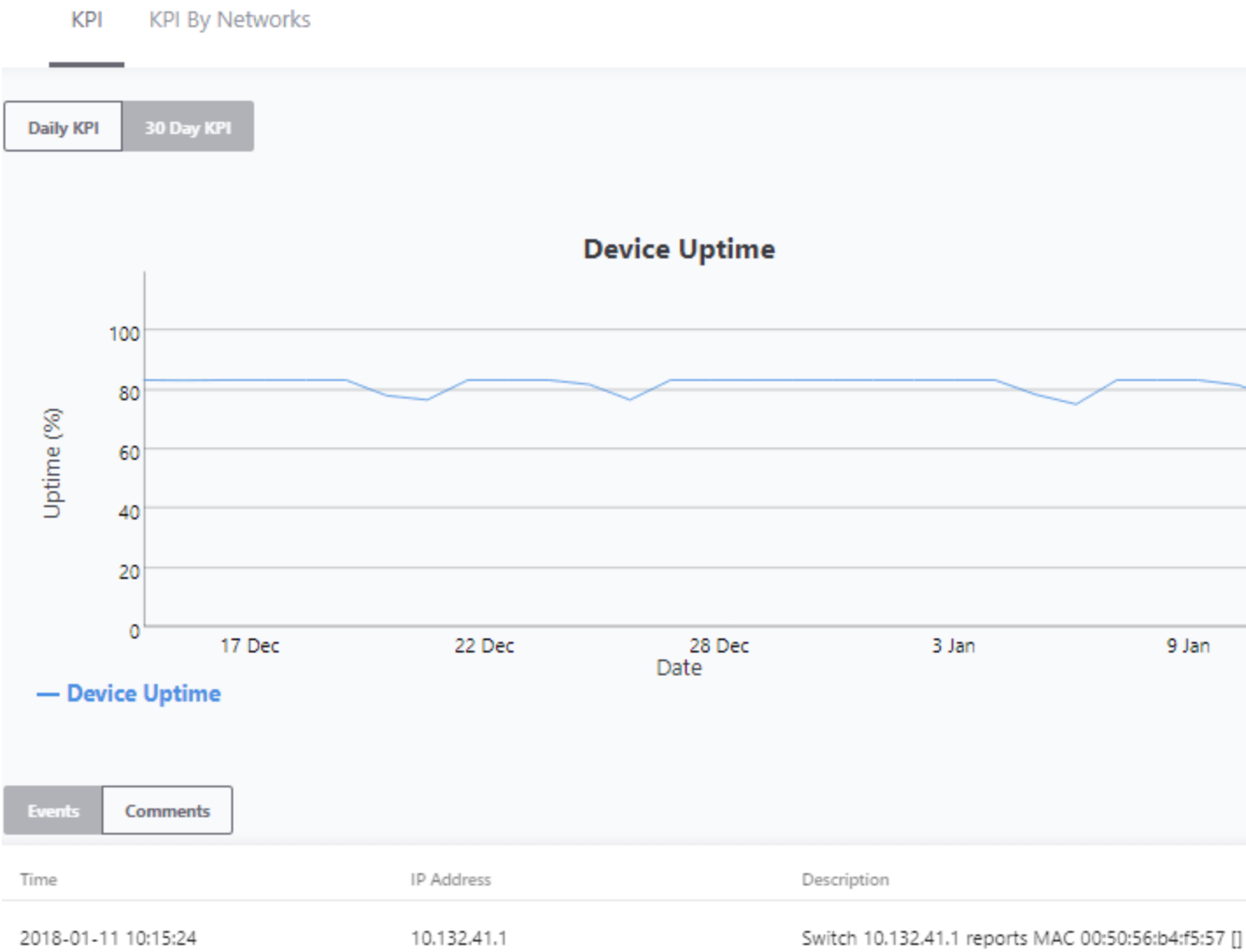
On the right are the actual (msec) values used in creating the bar charts as well as telling you when the best and worst days occurred.

At the bottom of the report are the events that were considered as incidents so you can identify which critical devices are causing issues.

You may also view Comments instead of Events. When logged in you can add comments in this page by going to Comment > Add Comment > and click **OK** when finished.

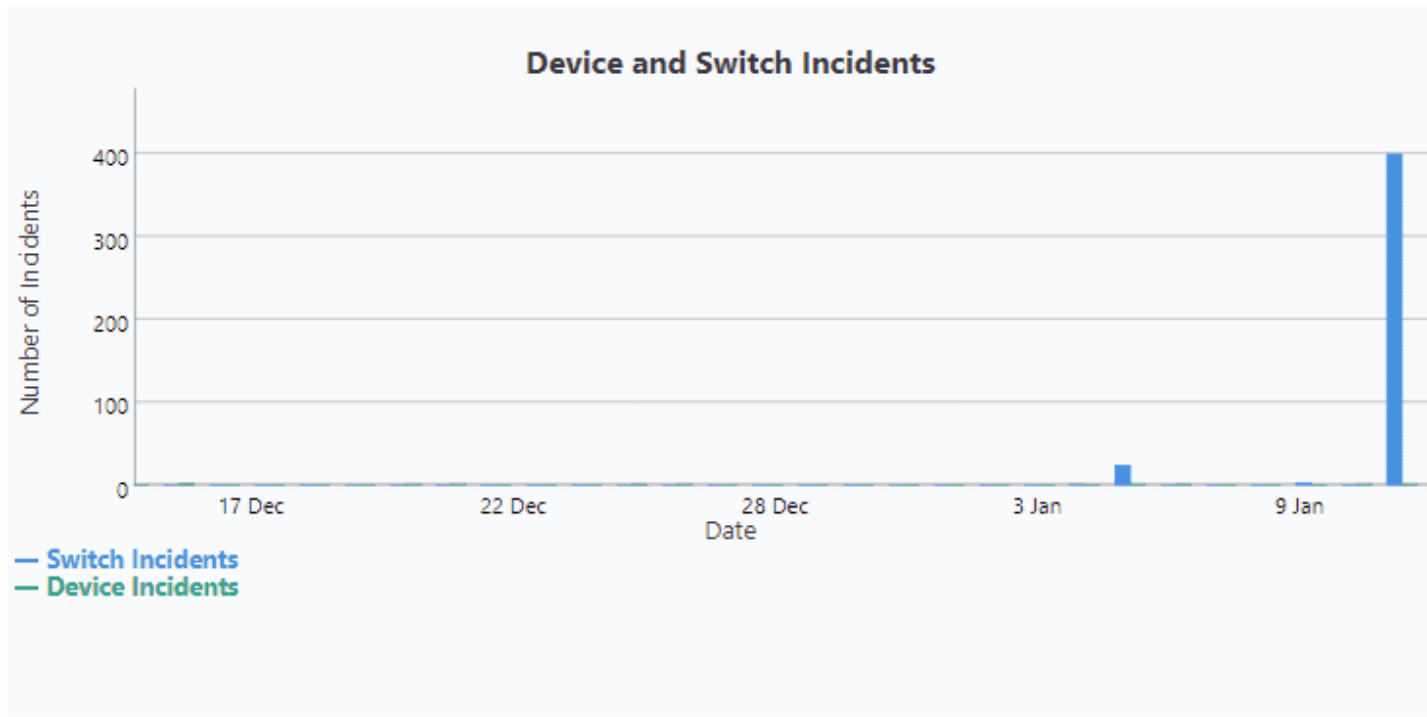
### 30 Day KPIs

**Device Uptime:** The 30 Day KPIs report provides you with the total device and switch incidents for each 24 hours over the last 30 days.



**Device and Switch Incidents:** Provide the Uptime percentage for the Critical Always On devices on a daily basis.

For this report a 'day' is a 24 hour period starting at the time the report is generated, not at mid-night.



Similar to the Daily Report, at the bottom is a list of events that make up the statistics.

### KPI By Networks

This view provides a high level summary of how each IntraVUE™ network is performing. The view has columns for data related to uptime and incidents reported in the last thirty days. The view can also be sorted in ascending or descending order for any column.

**KPI By Networks-** shows the cumulative KPIs for each IntraVUE™ network

**Details By Selected Network-** shows the KPIs just for that IP address. "No Data Available" appears whenever you have not selected an IntraVUE™ network above, or there are no devices found.

KPI By Networks										
Network Name	Uptime	Avg Uptime	Max Uptime	Min Uptime	Device Incidents	Avg Device Incidents	Max Device Incidents	Min Device Incidents	Switch Incidents	Avg Switch Incidents
56	76.30	80.02	81.57	76.11	0	14.8	36	0	8	8.7
192	100.00	99.79	100.00	97.39	24	23.8	54	2	22	21.2
57	100.00	65.15	100.00	7.69	2	4.2	12	0	10	8.6
58	80.95	68.90	80.95	61.57	0	1.8	16	0	18	17.6
59	52.62	53.16	57.89	47.37	1	0.3	2	0	8	5.1
37	3.13	3.11	3.13	2.99	0	0	0	0	2	2.0
41	37.48	36.71	37.48	31.69	0	1.8	27	0	8	5.1

Details by Selected Network										
Network Name	IP Address	Type	Critical Status	Admin Verified	Uptime	Avg Uptime	Max Uptime	Min Uptime	Incidents	Avg Incidents
56	<a href="#">10.132.56.113</a>	Device	Always On	No	100.00	99.89	100.00	97.40	0	0.2
56	<a href="#">10.132.56.83</a>	Device	Always On	Yes	100.00	100.00	100.00	100.00	0	0.1
56	<a href="#">10.132.56.10</a>	Device	Always On	No	100.00	100.00	100.00	99.96	0	0.0
56	<a href="#">10.132.56.16</a>	Device	Always On	Yes	99.85	99.23	99.91	96.63	0	0.2
56	<a href="#">10.132.56.12</a>	Device	Always On	Yes	100.00	99.99	100.00	99.95	0	0.1
56	<a href="#">10.132.56.13</a>	Device	Always On	Yes	99.97	100.00	100.00	99.97	0	0.6
56	<a href="#">10.132.56.11</a>	Device	Always On	Yes	100.00	100.00	100.00	99.97	0	0.2



Selecting the IP address of a device on the section "Details by Selected Network" will center that device in the Topology View.

See the Glossary to understand what each data value means.

## Export List

A new feature allowing a user to export a file by the .csv file is available for **KPI by Networks** and **Details by Selected Network**.

## IntraVUE Automated Diagnostic Reports

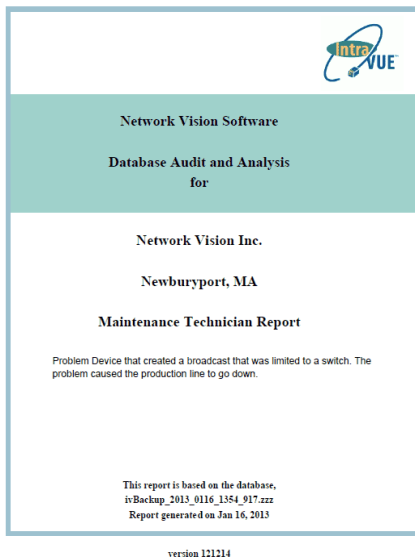
As Ethernet expands and is deployed into the heart of many Automation applications it will require Electricians and Technicians to have methods to maintain and support them. Most first responders are not individuals that will sit in front of a screen trying to understand the meaning of graphs and charts. Their job is to periodically check to make sure everything is running or if there is a problem to get details on the location of the problem and what to do to resolve it. They may be the only person at a location and are looking for suggestions on what to look at, and instructions on how to

resolve an issue.

For others, there will be a need for a method to help interpret the collected data and automate the analysis to provide additional assistance. This can be used for many reasons such as help when initially configuring the system, periodic maintenance reviews, or if a disruption should occur that is not easily depicted in the displays.

IntraVUE Reports are an additional capability of IntraVUE that will automatically generate written reports that identifies the issues as well as suggested courses of action for many common problems that can occur on Industrial Ethernet Networks. They can be generated in minutes and contain the latest data contained in the IntraVUE system.

Reports will be divided into several categories and generated separately which focus on different areas as well as intended users:



- \* Configuration Analysis (Assessing any configuration issues)
- \* Critical Devices Report (Asset Management with history)
- \* Maintenance Technician Report (Electricians & Technicians)

The Report Generator will take advantage of the recording capability of IntraVUE in which time based details are logged in a relational database. The Report Generator duplicates and automates the processes of our support engineer's analytical procedures to interpret the data in order to provide

accurate assessments in minutes. This is a written report with identified the specific issues with devices and recommendations for a course of action to solve the problem.

See **Generate Analytics Reports** in [Completing Initial Configuration](#)

Diagnostics and Troubleshooting



Start with an IntraVUE Automated Analytics Report to rapidly drill down to root cause

Problem	How IntraVUE identifies the problem
Duplicate IP and	IntraVUE will mark an IP address that appear sin two locations with

MAC addresses	a red box. Bringing up the event log for that device will show two MAC addresses alternating between the same IP address. This will identify the location for both devices as well as the time at which it began.
Degraded or Damaged Physical Connection or EMI	Ping failure percentages can be trended in a graphed to identify if there are connection problems. These graphs can help pinpoint the time and frequency of failures that help identify the potential causes. These can be created from environmental issues such as vibration or electrical noise from a large motor.
Insufficient Bandwidth	Look at Transmit and Receive bandwidth in threshold graphs, which show up as a percentage of available bandwidth.
Periodic bursts in traffic / Broadcast storm	When bandwidth shows greater than 75% utilization, there is risk to the performance of the network. Use the transmit bandwidth graph - device only – to identify the source of the broadcast storm. Use “Receive bandwidth” graph, all devices – to identify the affected devices. These disturbances may also be seen in the main map view with yellow lines going to a switch and down to the devices due to traffic exceeded or Ping response times exceeded.
Port Speed / Duplex Mismatch	Intermittent connections can often be traced to port speed mismatch. Right-click on any connecting line and IntraVUE will identify existing communication speed of that port.
Foreign Devices connected to network	IntraVUE identifies new devices with a tan colored box which is differentiated from the admin verified blue colored boxes. A red line will indicate the device is no longer connected. The event log will provide details of when the device was connected to the network.
Accidental move to wrong switch port	The potential for a connection to be accidentally changed due to device additions or just servicing the switch is becoming more common. IntraVUE monitors the moves and provides a graphic indication if a device is moved. The Event Log will also identify the day

	and time the move occurred.
Device failure or automatic restarting	IntraVUE provides a live animated graphic that can show a disconnected device by a red line. A first check would be to see if the connection to the switch is still made. If so, the event log will show if there have been several intermittent disconnections prior to failure.
Bad RSTP, Ring Switches, or accidental cable loops	The event log will show IntraVUE oscillating between two links or report the same MAC addresses on two different ports. These disturbances may also be seen as the network constantly changing in the main map view.
Intermittent losses caused vibration, electrical noise, and moisture	In a good network there should be no ping failures. The ping % failures rate per minute can be trended to identify connection problems. The Multi-device threshold graphs can help pinpoint the time and frequency of failures that help identify potential causes.
Devices starting to degrade in performance	Constant "empty" spaces or drops in the application threshold graphs (Xmit BW and/or Recv BW) but not in the communication physical threshold graphs (Ping failure / delay) indicate that a device is not sending or receiving traffic and troubleshooting or replacement is required. Verification can be done on the receiving device communication & application threshold graphs.
Large file transfers	These can be seen easily when looking at the transmit bandwidth and received bandwidth threshold graphs between two separate devices.
Communication module or switch lockups, power failures, or resets	A connection's properties can show trends of the transmitted / received data vs below ping response / ping failure percentages. A drop in data communication at the same time as ping failure at 100% can provides clues of this behavior.
Non-compliant device replacement, Device	A device properties can provide information such as vendor, model



### Deployment

number, and version of newly added devices. IntraVUE also automatically detects if a device has a web link, or provides means to add additional information in the device properties

## [Creating Plant Documentation](#)

### Creating Plant Documentation

Current device documentation does not reflect an up to date view of the plant network and a logical view makes it hard to keep up with relevant changes. These steps allow you to create current and relevant documentation for the IntraVUE plant network in logical format as well as in paper format.

#### Edit Device Properties

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click on any device. A slider bar will pop up on the right on the screen. This is your device properties panel.



If you haven't Admin Verified such devices click "Admin Verify". See [Admin Verification in IntraVUE 3](#)

3. While logged in as admin click "Edit". The Device Configuration dialog has 6 sections that allow you to configure the unique properties of a device.
-

<b>General</b>	^
<b>Other Names</b>	^
<b>Image</b>	^
<b>Advanced</b>	^
<b>SNMP</b>	^
<b>Links</b>	^

4. In the General Tab > Set a defined device name and location.
5. In the Other Names tab > Set additional defined names (i.e. function, description, owner ).
6. In the Image tab > Assign an image from the drop down.
7. In the Links tab > Fill in any documentation link (e.g. Administration Web link, Floor Layout, Maintenance user manual, wiring diagram, location pictures, various devices properties) for each URL NAME box that wasn't auto-detected by IntraVUE.
8. Click " Apply and Close"



Remember to save your changes before clicking on a different device as your changes will not be saved automatically.

9. Continue doing this for all end devices, switches, and the top parents (i.e. router, IntraVUE™ agent, and the IntraVUE™ host).

Tab	Description
General	Contains Admin Verification, wireless, SNMP, email, and other settings. See <a href="#">Device Configure - General</a>
Other Names	Allows you to set other devices names in the devices properties. See <a href="#">Device Configure - Other Names</a>

Image	Allows you to assign an image to a device. See <a href="#">Device Configuration - Image</a>
Advanced	Allows you to change device type and behavior on the map view. See <a href="#">Device Configuration - Advanced Tab</a>
SNMP	Allows you to enable or disable SNMP requests to a device. See <a href="#">Device Configure - SNMP</a>
Links	Allows you to assign Web Links to a device. See <a href="#">Device Configure - Links</a>



Refer to [Side View in Edit Mode](#) for detailed explanations for all device properties

---

## Multi-Device Configuration Export

### Import & Export Functions - CSV File

When you look at the exported data in a spreadsheet program you will find many columns. There are 3 basic sections:

- » Reference data
- » Configuration data for each IntraVUE™ 'View'
- » Configuration data from the device's General Tab
- » When saving the file, use CSV as the type and use quotes as the field marker. Don't use quotes in any view names.

Although the export function outputs many columns, you may delete columns you are not interested in EXCEPT the ipAddress, ref, and parentRef columns. These are used during the import process. You may not change any values to the left of DeviceName. They are shown in the image below.

---

	A	B	C	D	E	F	G	H	
1	IP	Active	MAC	Ref	ParentRef	ParentIP	ParentPort	UplinkPort	Devi
2	10.2.2.1	1	00 00 0C 07 AC 00	5	1		0	0	stsw
3	10.2.2.5	1	00 80 63 08 CF 3E	232	5	10.2.2.1	23	1	Hirso
4	n/a	1		256	232	10.2.2.5	7	0	Auto
5	10.2.2.251	1	00 20 B7 00 18 9A	236	256	n/a	0	0	no n
6	10.2.2.252	1	00 20 B7 00 18 9E	238	256	n/a	0	0	no n
7	10.1.1.88	1	00 01 02 6F A2 70	9	1		0	0	WHI
8	192.168.100.2	1	00 0C 29 3C 97 2A	67	9	10.1.1.88	0	0	vm-u

- » IP - IP Address or n/a if the line represents an auto inserted node.
- » Active - 1 if the device is currently connected.
- » MAC - MAC Address.
- » Ref - internal database reference number.
- » ParentRef - internal database reference of the device's parent.
- » ParentIP - The IP Address of the device's parent. This will be a switch, router, or the top parent of the IntraVUE™ network.
- » ParentPort - The port number from the parent to the device.
- » UlinkPort - If the parent is a switch, the uplink is the port leading back to the top parent, otherwise it is 0.

It is particularly useful to SORT the exported data by the ParentIP column and then by the ParentPort column. This will give you a list of all your devices arranged by the switch they are connected to, in port number sequence. This is very useful if you want to compare what IntraVUE™ says to what your documentation says.

The next section contains contains columns for names, weblinks, and images. There is one subsection for each of the 6 views of IntraVUE™. Note there is no column for IP View Name because you can not change that.



- » Category
- » Auto Connect
- » AutoBootp
- » IsWireless - this corresponds to the WAP checkbox.
- » Send Alarms - to 'this' device's specific recipient.
- » AlarmEmailAddress - email for 'this' device's specific recipient.
- » SendToDefaultUser- to email alarm recipient in the System Configure Email tab.
- » Verified - Admin Verified checkbox.
- » Properties - An encapsulation of several items on the Device's General Tab. This column is not meant to be edited. It is meant to be copied from one device configured the way you want to another device without modification. This includes columns such as 'disable all snmp', 'ignore bridge mib', 'use snmp for mac', and snmp community.
- » PKI.critical - This column is only available when you have enabled critical status for the KPI System on at least one device. See [Device Configure - General](#)

See [CSV Column Values](#) for a list of available values for selected columns

Refer to [Export / Import](#) for more options

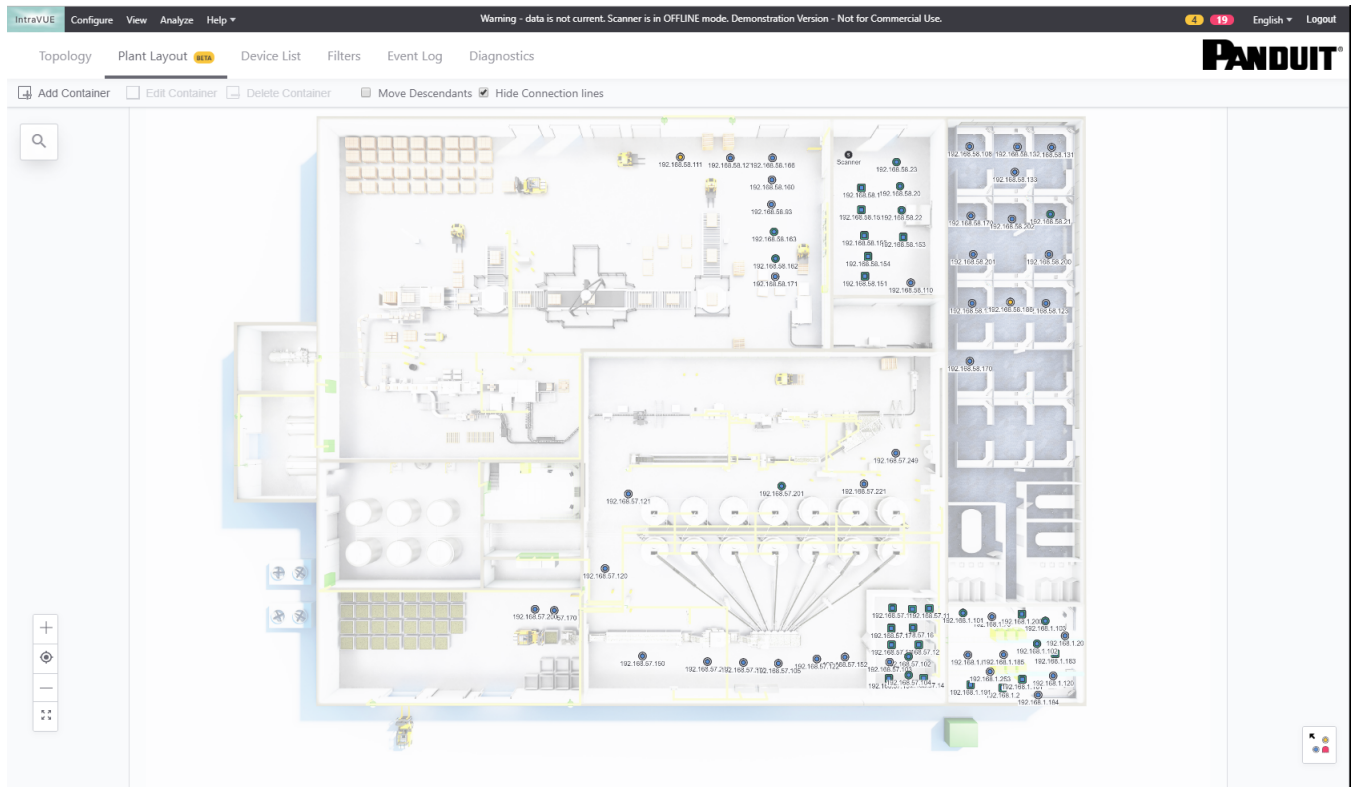
---

### Plant Layout View

With this new feature under the Configure tab, you are able to manipulate the Topology view of your network to your individual requirements, draw individual zones or "containers" to re-arrange your network, and print the entire plant layout with or without a background plant diagram in various sizes. This steps requires you already have IntraVUE™ scanning a network (see [Completing Initial Configuration](#)).

The new feature included a Remove option to remove images from the Plant Layout and a Reset Layout Devices button when completed.

---



Follow these steps to print a plant layout of your current plant network topology:

1. Open a IntraVUE™ by going to <http://127.0.0.1:8765> or <https://127.0.0.1:8766> (when HTTPS is enabled) on your browser. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click **Configure** and **Plant Layout**.
3. Click **Login to Continue** and enter the user name 'admin' and password 'intravue' in the default account.
4. A preview appears. You have two choices:
  1. Load a background layout image:
    - a. If you have a professional image (\*JPG, PNG, or GIF less than 10MB) click "Choose File" and browse to the location of that image. Sample images are under C:\intravue\plant\_layout

1. Click 'Open' to preview the image.
    2. Click on "Select a Size" (see that chart in step 9 below to see the exact dimensions). ANSI D is the most popular.
    3. Click 'Submit' to apply an image to the Plant Layout view
  2. Skip loading an image: Click "Cancel" and go to # 5.
  5. The Plant Layout has multiple Functions and Settings
    1. You can zoom in and out by using your mouse roller or by clicking the view controls on the far left bottom of the screen.
    2. You can move the entire topology to include areas outside of the screen area by dragging the topology with a left-click hold with your mouse.
    3. You can move any node around a 365 degrees motion by doing a left-click hold with your mouse and drag the node.
    4. To move a parent node and children:
      - a. Hold both the C-trl and 'x' keys and do a left-click hold with your mouse to draw an area around the devices you want to move. The devices in the drawn area will be highlighted. Do a left-click + hold drag to move the selected devices to the desired location.
      - b. OR. Click setting "Move Descendants" and simply left-click hold drag the parent node and children to the desired location. Uncheck this option to prevent nodes with children to be moved accidentally.
      - c. You will see that the connection lines disappear while moving the device.
  5. Plant layout comes with containers that you can use to specify which devices are in a different zone in the plant (e.g. a different floor, room, or cabinet). To create containers:
    - a. Click "Add Container". The label will turn blue
    - b. Hold the Ctrl key and click + drag the left mouse diagonally to draw a container around devices. You will be prompted to provide a name for the container
-



before it can be created. You can create more containers while the "Add Container" option is enabled.

- c. To expand, or shrink a container by doing a single left click on it and resizing it. To move a container, click on the "Add Container" button. The button will turn back to black color.
- d. Subsequent containers will be numbered in sequence starting with "Area 1".
- e. Double click on a container to automatically zoom in.
- f. To delete a container click do a single left click and then click "Delete Container". Repeat this step to delete subsequent containers.

6. To replace or remove the background image:

- 1. Click on "Edit Workspace"
- 2. Click 'Remove' to remove the background image. The Preview will become blank.
  - 1. To have a blank background select a size and click 'Submit' without choosing a file.
- 3. To pick another background image click "Choose File", select a size, and click 'Submit'

- 7. Device position and containers will be automatically saved to the currently used IntraVUE database and are available if you copy the database to another IntraVUE™ host. You will have to repeat step 4 above if you want to see the same plant layout on a different IntraVUE™ host.
- 8. A "New Changes Applied" banner in green letters will appear on the left side of the plant view constantly as you make changes. If you tab over to the Topology view and back you will notice the changes are saved.
- 9. The plant layout can be printed in both ANSI (American) paper sizes or ISO A0-A4 (International) paper sizes.

Size	Width x Height (mm)	Width x Height (in)	Closest ISO
------	---------------------	---------------------	-------------

<b>ANSI A</b>	216 x 279 mm	8.5 x 11 in	<b>A4</b>
<b>ANSI B</b>	279 x 432 mm	11 x 17 in	<b>A3</b>
<b>ANSI C</b>	432 x 559 mm	17 x 22 in (Requires a Plotter)	<b>A2</b>
<b>ANSI D</b>	559 x 864 mm	22 x 34 in (Requires a Plotter)	<b>A1</b>
<b>ANSI E</b>	864 x 1118 mm	34 x 44 (Requires a Plotter)	<b>A0</b>
<b>ISO A0</b>	841 x 1189 mm	33.1 x 46.8 in (Requires a Plotter)	<b>ANSI E</b>
<b>ISO A1</b>	594 x 841 mm	23.4 x 33.1 in (Requires a Plotter)	<b>ANSI D</b>
<b>ISO A2</b>	420 x 594 mm	16.5 x 23.4 in (Requires a Plotter)	<b>ANSI C</b>
<b>ISO A3</b>	297 x 420 mm	11.7 x 16.5 in	<b>ANSI B</b>
<b>ISO A4</b>	210 x 297 mm	8.3 x 11.7 in	<b>ANSI A</b>

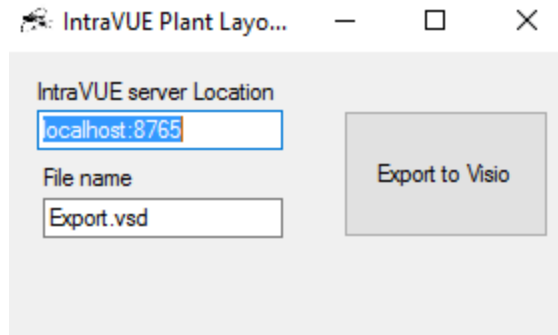
10. Print Plant Layout. To print the layout you have two options:

1. Print from Browser:

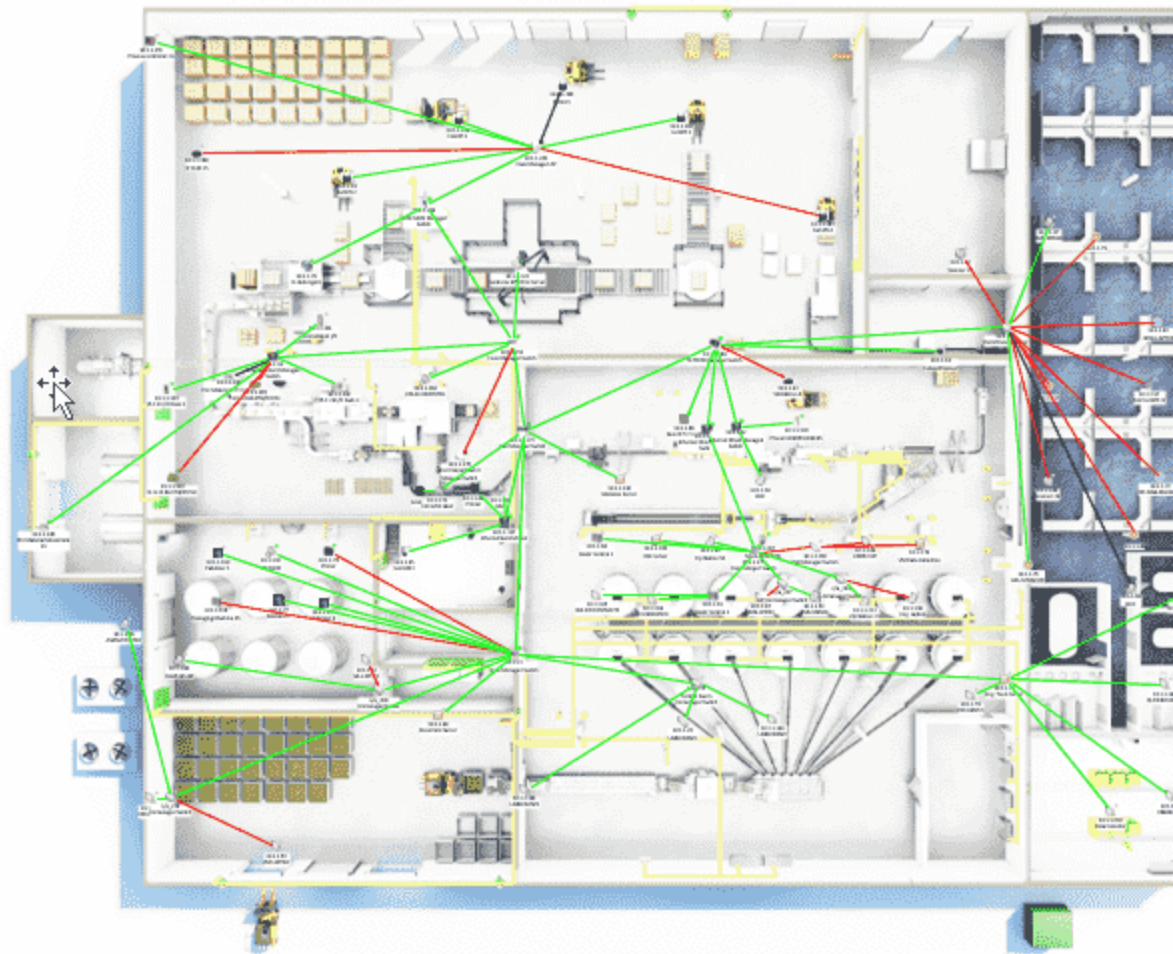
- a. Hit the Ctrl + P keys
- b. Select the desired paper size on your printer options. See step 9 above. Click 'Print'.
- c. Your final plant layout should look something like this

2. Visio Export + Print:

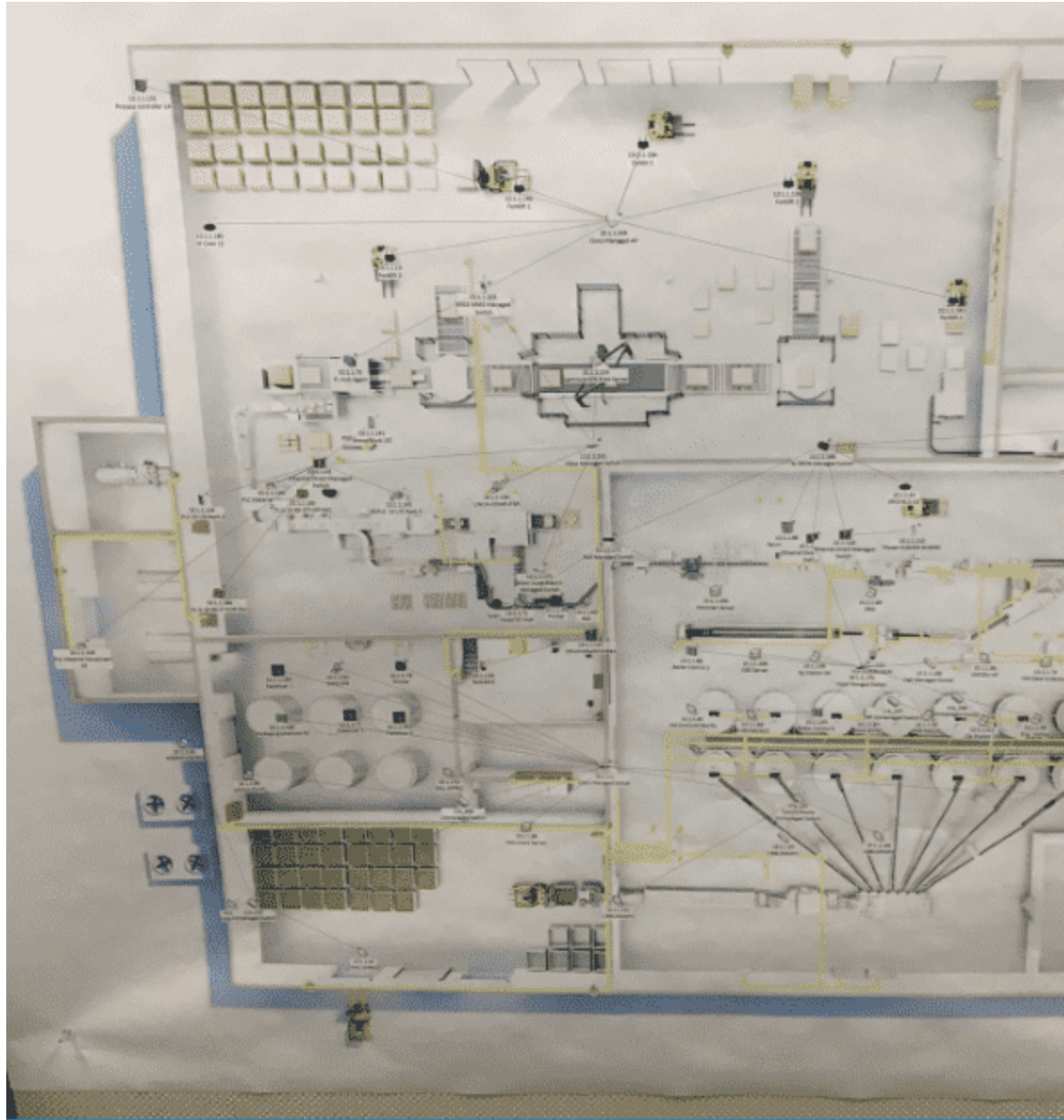
- a. Make sure you have the Visio package installed (i.e. Visio 2013 or 2016)
- b. Download the IntraVUE Plant Layout Export Tool ([IntraVUEPlantLayoutExporter.msi](#)). Run the installer and follow all prompts.
- c. Open the Plant Layout Export Tool from Start > Programs > IntraVUE Plant Layout Exporter



- d. Change the 'localhost:8765' to be x.x.x.x:8765 when running IntraVUE™ remotely. Change the File name as necessary and click "Export to Visio"
  - e. Wait for the Plant Layout too to change from "Processing..." to "Export Completed Successfully" and click on the 'x' to close.
  - f. Open the \*Export.vsd file. It should look something like the following image:
-



- g. Hit the Ctrl + P keys
- h. Select the desired paper size on your printer options. We selected ISO A0 for this example. See step 9 above. Click 'Print'
- i. Mount this plant layout on a wall or provide to your integrator.

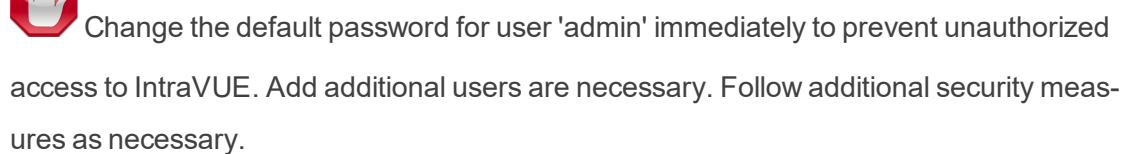


---

## Completing Initial Configuration

At the end of these steps your IntraVUE™ network(s) should look similar to this image.

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click on "Configuration", sign in as an "admin".





Failure to enable SNMP read-only (RO) community on the managed routers & switches results in **Unresolved Nodes**<sup>1</sup>. See IntraVUE Requirements in [Installation & Registration](#) before continuing.

3. Scan Speed: the speed of the IntraVUE™ scan engine (how fast IntraVUE packets are put on the network) can be conveniently adjusted with the Scan Speed control buttons. See [Configure Menu - Scanner Tab](#)



**Alert:** Some very old Ethernet devices, e.g. PCL 5/40, may misbehave or reset when using Fast & Ultra scanner speed settings when not using the recommended setting, or when other scanning software is running in parallel on the same automation network. Check with Panduit IntraVUE Support to learn more before attempting to increase Scanner speed above the "Slow" value.

4. Add IntraVUE™ Networks under "Network Configuration".
3. Click 'Add' to create a new network
  1. Give it a meaningful name such as "PLCX" or "Conveyor Y"
  2. Give it the IP address of the **Top Parent**<sup>2</sup>:



See [Selecting The Top Parent](#) for an explanation about the importance of the top parent IP address.

---

---

<sup>1</sup>Devices under the Unresolved node will have all the functionality of other devices in IntraVUE. The Unresolved node serves as a placeholder for devices that can not be properly placed by IntraVUE with some information indicating the difficulty.

<sup>2</sup>The device that can provide the mac addresses for IP addresses in a network.

---

### 3. Select what to scan:

1. Scanning the Local Plant Network using the IntraVUE™ host:
  - a. Check "USE LOCAL COMPUTER" and select one of the interfaces on the IntraVUE host itself.
  - b. The scan range will auto populate based on the top parent's IP address. A class C IP address range is suggested but can be larger.
  - c. Enter additional scan ranges that can be pinged from the IntraVUE™ host
  - d. Click "Save & Scan Network" to save changes
  - e.

NETWORK NAME	USE LOCAL COMPUTER	TOP PARENT	SCAN RANGE
VLAN 1	<input checked="" type="checkbox"/>	192.168.174.1	192.168.174.1
			Add Range
Add Network			

### 2. Scanning a routable network (or VLAN) using the IntraVUE™ host:

1. Enter the gateway IP address of that routable network (i.e. typically the .1 address) as top parent
2. The scan range will auto populate based on the top parent's IP address. A class C IP address range is suggested but can be larger.



It is important to include in the scan range section the IP addresses of all of the fully managed switches in either or both the local, remote, and isolated networks. This is required for IntraVUE™ to do a cross matching of IP to MAC address and position the IP device on its actual physical location on the topology map.



3. Enter additional scan ranges that can be pinged from the IntraVUE™ host
4. Click "Save & Scan Network" to save changes

NETWORK NAME	TOP PARENT	SCAN RANGE	
VLAN30 - Cable Ties	10.132.58.1	10.132.58.1	10.132.58.2
		10.132.57.1	10.132.57.2
		Add Range	

Remove Network

3. Scanning an un-routable network or isolated remote network using the IntraVUE™ Appliance as an Agent.
  1. Enter the designated IP address of the uplink port (typically LAN 1/IP1) of the IntraVUE™ Agent as the top parent
  2. Enter the IP address scan range of the isolated network(s) in both boxes of the scan range section
  3. Click "Save & Scan Network" to save changes

NETWORK NAME	TOP PARENT	SCAN RANGE	
PLCs	10.132.58.170	192.168.1.1	192.168.1.254
		10.132.58.170	10.132.58.170
		Add Range	

Remove Network



When adding multiple networks, make sure fill out all fields for each subsequent network in order to get prompted to "Save & Scan Network".

5. IntraVUE will now begin scanning. Click on "View" on the top navigation menu to return to the Topology view and see scanning discovery process.
6. Allow a few minutes (depending on the number of nodes) for IntraVUE to start building your network topology.

---

### Fine Tuning

When new devices are added the IntraVUE Scanner will spend several minutes developing the Network Topology. Viewing at this time will not provide an accurate depiction of the topology.

Initially IntraVUE will show all discovered devices linked to a special Unresolved node connected to the top parent.



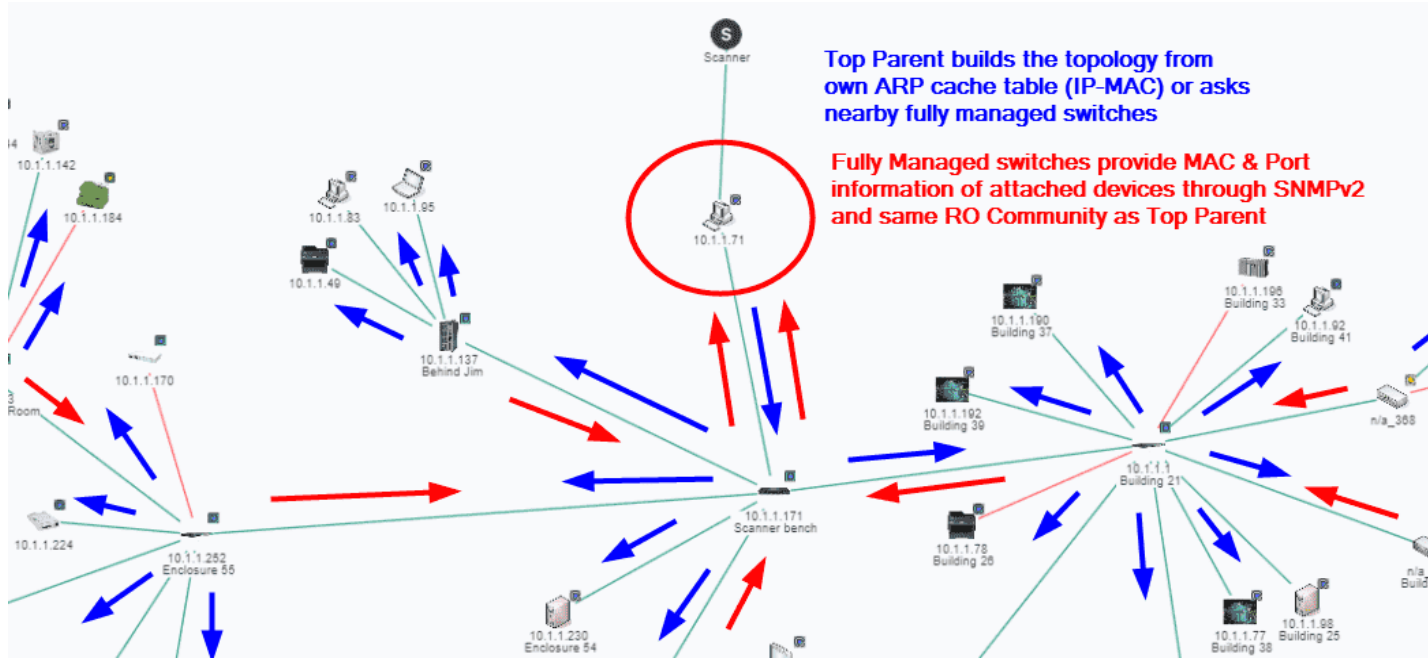
As soon as a device responds to a ping it is placed under the Unresolved Devices node and the individual nodes. During this period IntraVUE first attempts to find MAC address information from the top parent and any local routers or layer 3 switch.



One cause of IntraVUE not determining the MAC address is an incorrect or missing SNMP read-only community setting in a managed router's own configuration, or in the IntraVUE System Configuration Scanner's tab, "Default SNMP Read Only community". This is usually set to 'public'.

Once the MAC address has been determined, IntraVUE attempts to find the correct location in the network hierarchy to place the device.

---



If the IP of the device is in the same subnet as the top parent it will be moved to the top parent pending a move to a managed switch. If it is in a different subnet from the top parent of that Intravue network, it will remain in unresolved unless a router having an interface for that IP is discovered or a managed switch claims its mac address on a port. In those cases the device will move out of unresolved. This situation could occur due to an incorrect community in a router or switch, or its switch is not in the scan range.

Devices under the Unresolved node will have all the functionality of other devices in IntraVUE. The Unresolved node serves as a placeholder for devices that can not be properly placed by IntraVUE with some information indicating the difficulty. See also [Selecting The Top Parent](#).

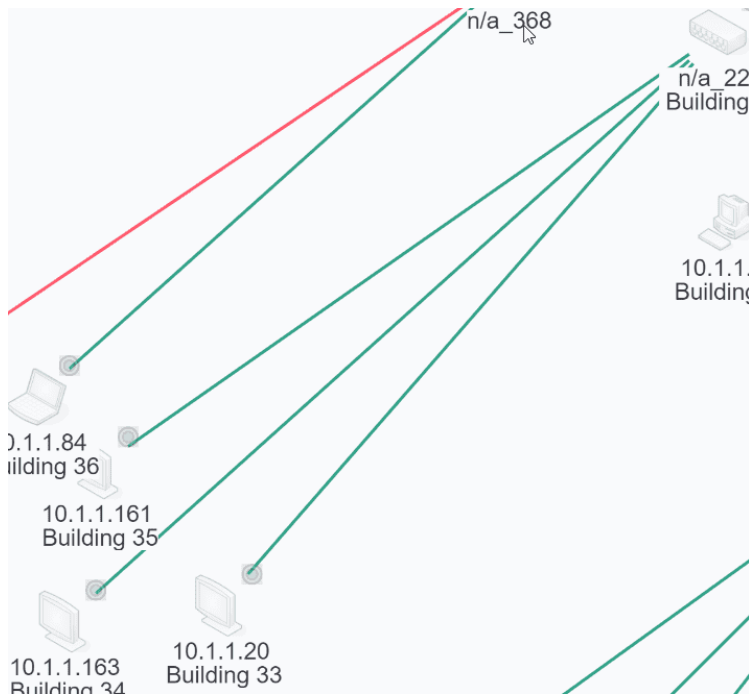
In the case that switches in a different subnet can not provide MAC information because of lack of access to SNMP on router that bridges the other subnet, you can enable the option "Use SNMP provided MAC" which will provide the MAC address from the SNMP of the switch. See also [Device Configure - SNMP](#).

### n/a Nodes

An unmanaged switch that has an IP address but which does not support SNMP will be found and displayed under an auto-inserted node along with the devices that are directly connected to the switch. This is because they will all be found on the same port of the unmanaged switch's parent

and any lower down managed switches will see them on the 'uplink' port back toward the IntraVUE™ host.

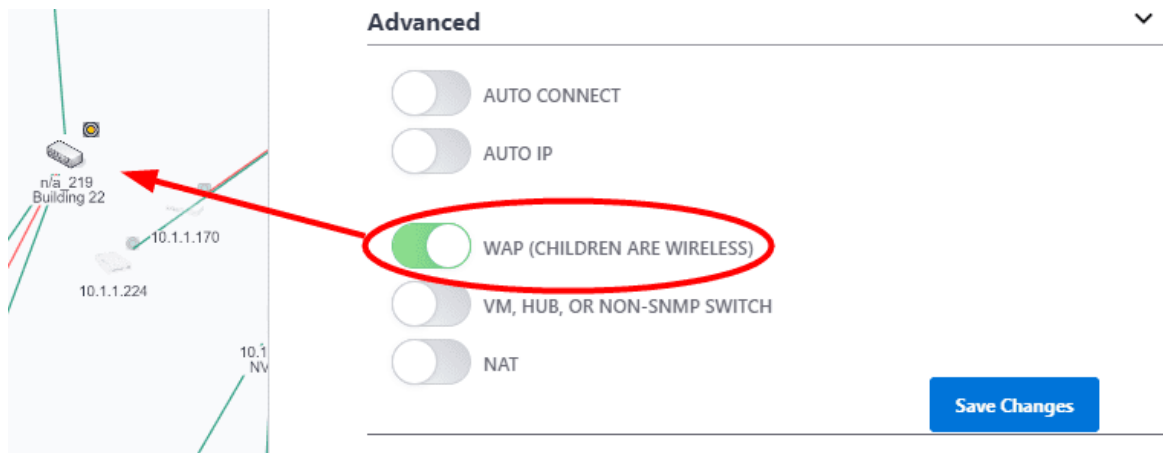
The image below shows the way IntraVUE™ will display an unmanaged switch that has an IP address having two devices connected to it. If a managed switch does not have its SNMP community set correctly it will appear the same. The 10.1.1.163 device is an unmanaged switch with the .161 and .20 devices physically attached.



The parent managed switch of these devices reports them all on the same port, so IntraVUE™ automatically inserts a node, labeled 'n/a' to represent the hub or unmanaged switch which must be present.

To learn the difference between 'n/a' nodes and 'N/A' nodes see [NA Nodes](#) for more details.

In order to show the network as it physically exists the administrator can select the Configure item from the unmanaged switches Device Menu. Check the checkbox 'Unmanaged Switch or Wireless AP' or 'Virtual Machine, Web Managed Switch, Access Point' on newer IntraVUE versions. Click 'Save Changes'.



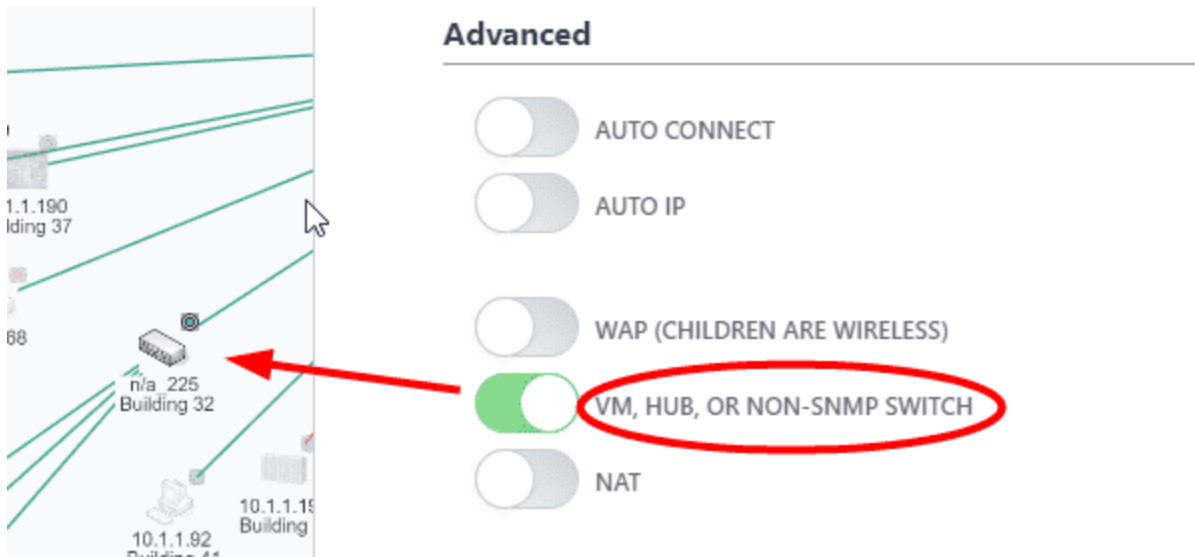
After a minute, the auto inserted node will go away as there is now only one device on the port of the managed switch and the other two devices are below it.



Some old unmanaged switches and hubs don't have a IP address by default or because of missing configuration. IntraVUE will not be able to see these without an IP address. In order to show the network as it physically exists you can add child nodes and move attached devices under this unmanaged switch. This is not recommended as monitoring for that switch is very limited.

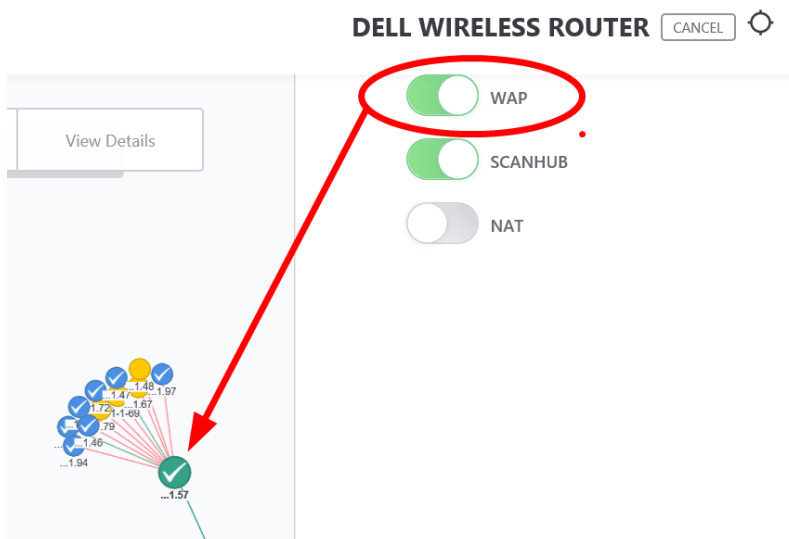
## Virtual Machines

Similar to unmanaged switches, a virtual hosts server will display an 'n/a' node with devices physically attached it. In order to show the network as it physically exists the administrator can select the 'Configure' item from the virtual machine's Device Menu. Check 'Virtual Machine, Web Managed Switch, Access Point' and then Click 'Save Changes'. After a minute, the auto inserted node will go away as there is now only one device as the virtual host and the other devices are below it.



### Wireless Access Points (WAP)

Managed Wireless APs should be discovered by IntraVUE™ and will automatically get the checkbox for 'Virtual Machine, Web Managed Switch, Access Point' in the Device Configure dialog checked. If you have a Wireless AP that is not managed, you can check the checkbox yourself.



The result will be that all wireless devices will appear under the Wireless AP.

To identify the Wireless AP network better in the IntraVUE UI, you can check the 'WAP' checkbox and the child nodes will have dashed, wireless, lines going to them.

Refer to for more details

### Ring Networks

IntraVUE can map certain ring topologies as long as they are based on PROFINET or Ethernet/IP technology. DLR network topologies is the most common in which having each drive connecting from the first one to the last one back to the same EtherNet/IP nic card's port. The drives are fixed so they won't move around. See [Device \(DLR\) and Switch Level Ring Networks](#) for more details. Switch rings are not being detected currently by IntraVUE 3.1.

### Inconsistent Results

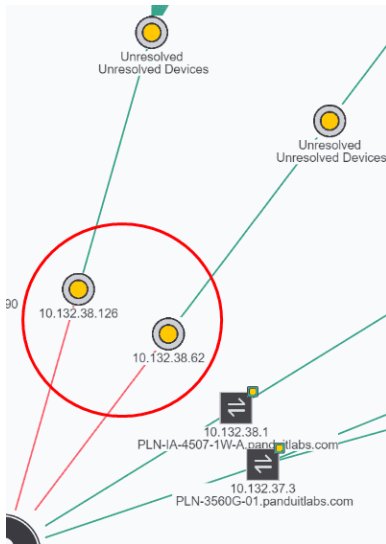


IntraVUE will only detect nodes that can be verified through a simple ping command in DOS.

- » Not seeing devices: disable active windows firewall rules on the IntraVUE host machine or ACLs on the network. See System Requirements in [Installation & Registration](#)
- » Missing devices or Topology no branching out correctly: See the [Selecting The Top Parent](#), & [Configure Menu - Scanner Tab](#)

### Disconnected Top Parent Nodes

---



Some Top Parents may appear as disconnected after being visualized.

These nodes would appear with a red connection while the rest of topology has a green connections. This does not affect scanning the rest of the topology but simply means that IntraVUE™ discovered a disconnected device.

If the disconnected device is a top parent node (e.g. a router or L3 Switch) simply reconnect that device back online, or select a top parent that it's live and can be reached by the IntraVUE™ server.

### Stopping IntraVUE because of presumed strange behavior in the Network

The IntraVUE Scanner works similarly to a SCADA scanner where it will ping the end devices without trying to write any information or causing them to malfunction.

IntraVUE will only report the health status of your network and never will try disrupt your network in any way, unless you have purposely set your scanner speed to 'Ultra' and you have very old automation devices.



It is always best to start scanning with the "Slow" scanner speed even if it takes longer to find devices. IntraVUE™ is known for scanning automation networks, but many times increasing the speed or having bad switches can react strangely and cause device issues around the same time IntraVUE™ is running. See "Known issues" under [FAQs](#)



---

### Connect IntraVUE & Key Performance Indicators

The **KPIs**<sup>1</sup> System on the next section requires that you set critical status for each device you want to get metrics for **Uptime**<sup>2</sup> and **Incidents**<sup>3</sup>. Critical Status is not required to finalize the initial configuration but we still encourage you to visit the next section "IntraVUE Analytics" for coverage on this topic. The Device List View shows the current state of KPI Critical Status for each node.

The Device List view is a report view that lets you see network information related to all devices visible in either the Topology or Plant Layout views.

- » IP Address: The IP of the Device
  - » Network Name: The IntraVUE network the device is configured with (See [Configure Menu - Scanner Tab](#))
  - » Device Name: From CIP or Netbios. Can be modified here (See below).
  - » Critical Status: See [Device Configure - General](#) & [IntraVUE Analytics](#). Can be modified here (See below).
  - » Admin Verified: See [Admin Verification in IntraVUE 3](#). Can be modified here (See below).
  - » Type: Device or Switch. Can be modified here (See below).
  - » Revision: e.g. ENETIP Rev 7.01. Can be modified here (See below).
  - » Vendor: e.g. Rockwell. Can be modified here (See below).
- 

---

<sup>1</sup>KPIs are assorted variables that organizations use to assess, analyze and track manufacturing processes. These performance measurements are commonly used to evaluate success in relation to OEE goals and objectives

<sup>2</sup>The portion of the OEE Metric that represents the percentage of scheduled time that a device is available to operate. Often referred to as Uptime

<sup>3</sup>Incidents includes all events that cause stop time on planned production for an appreciable length of time (typically minutes or hours). That is, incidents cause availability Loss from unplanned events (e.g. equipment failures). It is calculated like this: Availability = Run Time / Planned Production Time  
Run Time = Planned Production Time – Stop Time

---

- » Model. e.g. 1756-EN2TR. Can be modified here (See below).
- » Location: e.g. Electrical Room
- » User Defined 1. Custom field. See [Device Configure - Other Names](#)

IntraVUE <span>Configure View Analyze Help About</span> <span>Warning - data is not current. Scanner is in OFFLINE mode. Demonstration Version</span>					
Topology Plant Layout <span>BETA</span> Device List Filters Event Log Diagnostics					
<div> <div>Double-click field to adjust value</div> <div>Search by criteria</div> <div>Type to filter data...</div> </div>					
IP Address	Network Name	Device Name	Critical Status	Admin Verified	Type
10.1.1.71	Network 1	MARK-PC	Always On	Yes	Device
10.1.1.171	Network 1	Dell Managed Switch	Always On	Yes	Switch
10.1.1.137	Network 1	Ethernet Direct Managed Switch	Always On	Yes	Switch
10.1.1.49	Network 1	Printer	Always On	Yes	Device



Selecting the IP address of a device will center that device in the Topology View.

### Modify a Field directly from Device List View:

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Log in from the right-top corner using the default password "intravue".
3. By clicking on "Device List", you will see a list of all devices found.
4. Change the either Device Name or Critical Status by clicking double clicking on the actual value for that device until you notice that the value becomes editable. Most values are editable
5. When done click on an empty area away from the field until you get a blue "Save Changes" button. Click on it to save changes and move to the next row. Continue doing this for devices that need changes.

### Enabling Email Alarms

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click Configure to access the system menu and click on the “Email” tab.
3. Check the 'Enable Email' checkbox to activate email alarms.



Note that on a new scan checking this checkbox will not result in ANY emails being sent. That is because, by default, no device will have its 'Send Email to Default User' checked (See **Settings Required on Device Configuration** Below).

---

## EMAIL CONFIGURATION

Enable Email:



SECONDS TO WAIT FOR ALARM TO CLEAR BEFORE SENDING:

30

EMAIL ADDRESS TO SEND ALARMS TO:

control.engineer@myCompany.com

REPLY-TO ADDRESS IN EMAILS:

control.engineer@myCompany.com

EMAIL SERVER:

smtp.somewhere.com

SMTP PORT NUMBER:

25

Enable SMTP Authentication:



SMTP USERNAME:

jwmName

SMTP PASSWORD:

serverPassword

Enable Encryption:

[Test Email](#)[Apply](#)

4. The "SECONDS TO WAIT FOR ALARM TO CLEAR BEFORE SENDING" box sets the number of seconds an email alarm will be delayed before transmission. At the end of the delay time, IntraVUE will check to see if the alarm condition is still valid. If it is, the email will be sent at that time. 30 seconds is the default setting.
5. The "EMAIL ADDRESS TO SEND ALARMS TO" box field is the email address that will receive the email alarms for all devices. If there are more than one recipient you want to send emails alarms to separate each email address with a comma (e.g. user-1@company.com, user2@company.com, etc).
6. The "REPLY-TO ADDRESS IN EMAILS" box is required when your SMTP server requires a valid email address when emails are bounced back. It is also the reply to address that will be on the alarm emails (i.e. the "From" field). This email address may or may not have to be valid depending on your SMTP server.
7. The "EMAIL SERVER" requires the mail STMP server that will relay emails from IntraVUE™ to the email(s) on step 5 above.
8. The "SMTP PORT NUMBER" is necessary to connect to the SMTP server that will be relaying the email. Port 25 is the common.



It's best to use a company SMTP server as public SMTP servers (e.g. gmail or yahoo mail) could take a long time to receive alerts.

9. SMTP Authentication and Encryption are optional and not required by IntraVUE to sent alerts.
10. The "Test Email" button will will immediately generate a test email using the settings entered in the earlier steps. If you make a change, select the APPLY button before selecting "Test Email". This feature avoids having to disconnect a device just to test your email settings.

### Settings Required on Device Configuration

In the [Device Configure - General](#), click 'Edit', 'Send Alarms' button. This is NOT enabled by default. If enabled the default user (specified under Configure > Email) will get email alerts for this device.

---

There is also an 'Send Alarms to Default User' button. If you want an additional email sent to someone besides the default user, click this button AND edit the 'Alarm Email Address' field for the email of the person to get email alerts for this particular device.

☒ SEND ALARMS

ALARM EMAIL ADDRESS

×

☒ SEND ALARMS TO DEFAULT USER

### When the "Test Email" button does not work

When you use the Test Email button and you do not receive an answer, there will be some text in an Exception message indicating the specific cause of the failure. For instance refused by SMTP host, invalid user name or password, etc.

This message is found in the scanner log file located at ...\\intravue\\log and will be the ivserver\_(date)\_(time).out file at the time you pressed Test Email.

<p>A sample of what is generated. It was generated by doing a Test Email with the default Email Setup dialog. The stacktrace line "javax.mail.MessagingException: Unknown SMTP host: smtp.p.somewhere.com;" tells you that the SMTP host, the email service provider, is incorrect or that you can not connect to it.</p>	<pre>0120 100016 event: Device 10.1.1.67 reconnected 0120 100054 event: Device 10.1.1.90 moved from 10.1.1.244:9 to 10.1.1.16:2 0120 100054 event: deleted child node at 10.1.1.244:9 0120 100111 event: 10.1.1.32 Ping Response Threshold Exceeded 0120 100122 received mod request send test email 0 0 0120 100122 send test email 0120 100123 EmailTask runs: Intravue has been instructed by the admin to send a test email. Please see http://10.1.1.59:8765/ to [unused] 0120 100123 Unexpected Exception thrown - stacktrace follows: javax.mail.MessagingException: Unknown SMTP host: smtp.somewhere.com; nested excep- tion is: java.net.UnknownHostException: smt- p.somewhere.com at</pre>
---	--

```
com.sun.mail.smtp.SMTPTransport.openServer
(SMTPTransport.java:1211) at com.sun-
.mail.smtp.SMTPTransport.protocolConnect(SMTPTrans-
port.java:311) at javax.mail.Service.connect
(Service.java:233) at javax.mail.Service.connect(Ser-
vice.java:134) at javax.mail.Service.connect(Ser-
vice.java:86) at com.sun.mail.smtp.SMTPTransport.connect
(SMTPTransport.java:144) at javax.mail.Transport.send0
(Transport.java:150) at javax.mail.Transport.send(Trans-
port.java:80) at database.EmailTask.run(EmailTask.java:76)
at java.util.TimerThread.mainLoop(Unknown Source) at
java.util.TimerThread.run(Unknown Source) 0120 100146
device 10.1.1.67 disconnected 0120 100146 event: Device
10.1.1.67 disconnected 0120 100207 device 10.1.1.90 recon-
nected
```

## Email Alarm Types

IntraVUE™ will generate an email alarms for the following events:

- » Device x.x.x.x disconnected - See [Event Log Descriptions](#)
  - » Subject: "Intravue alarm ip=w.x.y.z"
  - » Body: "Intravue reports device w.x.y.z has disconnected. Please see IntraVUE™ Link"
- » Device x.x.x.x reconnected - See [Event Log Descriptions](#)
  - » Subject: "Intravue alarm ip=w.x.y.z"
  - » Body: "Intravue reports device w.x.y.z has reconnected. Please see IntraVUE™ Link"

## Customizing the Email Message

The email message that is sent to the user can be customized. See [The ivserver.properties File](#).

---

- » The email subject line can be customized to include the device name.
- » The email body for a device disconnected message can add the device name and link.
- » The ip address used to provide a link to the IntraVUE host can be changed to allow users requiring a proxy address rather than the real host address to reach the IntraVUE browser.

See for email settings and testing

## Generate Analytics Reports

The IntraVUE On-Demand System Analytics are an additional capability of IntraVUE that will automatically generate written reports that identify issues as well as suggested courses of action for many common problems that can occur on Industrial Ethernet Networks. They can be generated in minutes and contain the latest data contained in the IntraVUE system.

The IntraVUE On-Demand System Analytics provides you with a PDF report based on the analysis of your IntraVUE System available anytime 27/7/365\*.

Once an account is established you will be able to upload a Support Archive and get the resulting network analysis & diagnosis report. The process takes about a minute to upload, two - three minutes for analysis, and then the report will be emailed to you\*\*.

**Network Vision Software**

**Database Audit and Analysis**

**Network Vision Software**

**Newburyport, MA**

**Maintenance Technician**

Problem Device that created a broadcast that problem caused the production line to go down

This report is based on the data backup\_2013\_0116\_1354\_9  
Report generated on Jan 16,

version 121214

1 Analysis Summary

Time used for this report:

First scanner data time: 2010-01-04 17:00  
Last scanner data time: 2010-01-28 06:21

Number of days from first event to last scanner time: 24

Last Version of IntraVUE: 2.1.0e8  
Product Key: 3ALU3-XX03E-DA999-C2072-98963  
Node count limit: 1024

Runtime of Scanner.

This report will primarily use information from the last 30 days below show the actual time the IntraVUE scanner was run each period are also printed.

Time	Duration
2010-01-28 06:21	3 hours of 1 minute data
2010-01-28 03:21	3 hours of 1 minute data
2010-01-28 00:20	15 hours of 10 minute data
2010-01-26 18:20	15 hours of 10 minute data
2010-01-25 11:00	15 days of 2 hour data
2010-01-10 11:00	15 days of 2 hour data

page 4

3. VLAN680

NOTE: The connection and verification status are as of the time of the scan.

NOTE: All devices should be verified. This will provide improved device additions and moves.

C	V	Mac Address	Device Name
Connected	Known and Verified	00 17 95 49 BC 41	DNYTR1-SW1.rhstone.com
Disconnected	New or not Verified	00 17 95 6A 20 41	DNYTR2-SW1.rhstone.com
Wireless Connected	Move or conflict	00 17 95 69 A3 C1	DNYTR3-SW1.rhstone.com
Wireless Disconnected	Move or conflict	00 17 B0 3C D7 41	DNYTR4-SW1.rhstone.com
W - wireless access point		00 17 59 25 A3 C1	DNYTR5-SW1.rhstone.com
		00 17 B0 33 BB C1	DNYTR6-SW1.rhstone.com
		00 17 B0 3D 64 41	DNYTR7-SW1.rhstone.com
		00 17 95 69 90 41	DNYTR8-SW1.rhstone.com
		00 17 94 A3 91 C1	DNYTR9-SW1.rhstone.com
		00 17 95 6A 1F C1	DNYTR10-SW1.rhstone.com
		00 18 73 5A C6 C1	DNYTR11-SW1.rhstone.com
		00 17 95 C5 9C 41	DNYTR12-SW1.rhstone.com
		00 18 BA 3D 9B 41	DNYTR13-SW1.rhstone.com
		00 1C B0 81 34 C1	DNYTR14-SW1.rhstone.com
		00 19 06 80 E0 C1	DNYTR15-SW1.rhstone.com
		00 1C B1 90 99 C1	DNYTR16-SW1.rhstone.com

Device Information:

3.2. Configuration Review

This section will analyze the database to identify general configuration issues that may improve IntraVUE ability to provide better diagnostics. Any issues will appear as a 'Warning' and will include an 'Action Required' for proper deployment and to take full advantage of the IntraVUE diagnostics.

**WARNING: 100 per cent of the devices in this network are NOT Admin Verified.** Many IntraVUE features are enhanced when devices are Admin Verified and some analysis in this report is only done on Admin Verified devices.

**ACTION:** Try to verify all devices except suspicious and unknown devices.

**WARNING: 54 per cent of the devices in this network do not have names assigned in Device View.** The use of a name in addition to the IP address and MAC address will make it easier to identify the specific device. In addition to names the IntraVUE software allows other data to be associated with the device such as Location, Manufacturer, Model, Version or Serial number.

**ACTION:** You can add details in the IntraVUE system by either going to each device's Device Configuration or by using Export/Import and making changes in a spreadsheet.

Good: no unresolved node

Good: No auto-inserted nodes having a managed switch as a child.

Good: There are less than 5 devices in this network that are unverified, disconnected devices.

Good: There are no admin verified devices that have moved (red nodes).

3.3. General Network Details: VLAN680

3.3.1. Connection Issues

page 7

page 12



1. Create a support archive (i.e. \*.zzz file). See [Generate Support Archive](#)
2. Either use the "Send Archive" button (See [Generate Support Archive](#)) or click on the link below to be redirected to the Analytics Reports portal <http://in-travue.panduit.com:8765/IntravueAudit/AuditServlet>
3. Login to the IntraVUE Report Generator by entering your primary email address and password.



If this is your first time, enter your email address and desired password and click "New User" to register.

4. Enter Company Name, Location, Comments, Report Type (Maintenance for troubleshooting and Configuration Analysis for IP scan ranges),
5. Select which columns to show (e.g. MAC address, Vendor, Model). Click "Apply Data"
6. Select "Choose File" and browse to your \*.zzz file location & click 'Upload Archive For Analysis'. Wait "Success: archive uploaded" message.
7. Click "Analyze database and email results".
8. A message "The archive is being processed and the results will be emailed to you in minutes with the PDF report attached" would appear when done. You can start a new report\* or close your browser.
9. If you are not receiving diagnostics reports or can not login to the Analytics Reports portal contact [techsupport@panduit.com](mailto:techsupport@panduit.com).

*\*There's no limit on the number of Analytics Reports you can request.*

*\*\*IntraVUE Advanced Subscribers automatically get a remote assessment of the IntraVUE Plant Network from one of our IntraVUE experts who will review their On-Demand System Analytics & Diagnosis Report and discuss with you recommendations, suggestions, and potential solutions to prevent, improve, or resolve network issues.*

---

The IntraVUE Agent



Skip this step if you are using a only setting up a Software Package (SNMS / SNMA). This section only applies to customers that have purchased the IntraVUE Appliance.

### **The IntraVUE Agent**



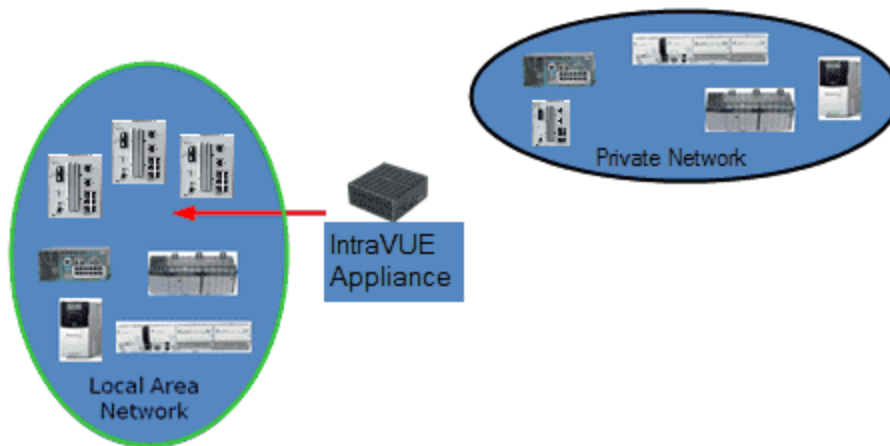
The IntraVUE Appliance is a small-factor headless appliance strategically placed in a network closet at a remote site with the purpose of scanning edge devices in one or multiple cases below:

1. Devices in an isolated network behind a gateway. A switch inside the 'isolated network' behind a gateway using one port of the agent and the other port of the agent is connected to a switch on the 'plant' side (or plant VLAN Access) network.
2. Private VLANs. One is the private VLAN of the 'system' and the other provides access from the 'plant' to the PLC of the 'system'. The IntraVUE Agent has one interface connected to a 'system VLAN' port of the switch and the other agent's Ethernet interface is connected to a 'plant VLAN' port of the same switch.
3. If a NAT, or Firewall Access to the NAT, or Firewall devices is configured to send all packets from an IP address on the plant side to the IP of the IntraVUE agent on the 'system' side of the NAT/Firewall, then the IntraVUE Agent can scan the devices behind the NAT, or Firewall.

### **Using IntraVUE Appliance as an Stand-alone Server to scan the Plant Network:**

When there is no physical server or virtual machine available, the small-factor headless appliance can be deployed as an IntraVUE Server. The only differences is that it does require software registration and only one port of the appliance is connected to a switch on the 'plant' side.

---



See [Using the IntraVUE Appliance as an Agent](#) for more details



See also [Using the IntraVUE Appliance as a Server](#) for more details



See [IntraVUE Appliance Configuration](#) for exact deployment and configuration steps

---

### Admin Verify Devices

Admin Verification is a process of establishing a controlled state of your network, or the devices which you are monitoring with IntraVUE.



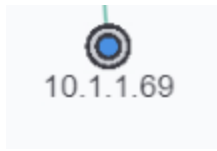
Rogue devices can be easily identified when all devices have been previously verified (see below) and when using device filters (see [View Filters](#))



Refer to [IntraVUE Legend](#) to understand node fill, outlines, and connecting line colors.

Each Admin Verified node has additional characteristics from a non-Verified node.

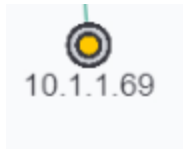
---



The node is normally blue filled.



If the position of the device changes the originally verified position becomes red filled.



The new position of the device becomes a tan filled node.



If the device that moved comes back to the original location, the tan filled node will go away and the red filled node will become blue filled again.



Failure to admin verify all of detected devices by IntraVUE will result in incomplete Analytics & KPIs Status Reports, missing configuration of newly detected devices, inability to detect when a device has moved or disconnected from ring or linear networks, and impairs your ability to identify what assets truly belong to your plant network and troubleshoot them accordingly.

When a node is tan filled it will stand out. It will call your attention to it. Find out what it is and then verify it or take some action to get the device off line.

A second tan filled node is the 'ghost' of the real position of a device. The real device will have a real IP name like 1.100.56 and the ghost node will have the IP 10-1-100-56.

If you see a tan filled node, find the corresponding tan filled node with dashes in the IP address.

If the new position is acceptable, delete the ghost tan filled node and admin verify the new position. In the future this two step process will become one step.

If the position is temporary, you may leave the red filled ghost. When the device is returned to its former position the red ghost will be replaced by a blue filled node.

To make Admin Verification easy, there is a single button that will automatically verify every device with an IP address that has not yet been verified. It's on the Scanner Tab of the [Configure Menu - Scanner Tab](#). See also [Device Configure - General](#) for verifying individual nodes.



Recommended: Take a snapshots of your database and user settings. Refer to

---

### [IntraVUE Analytics](#)

## Advanced

## Administration

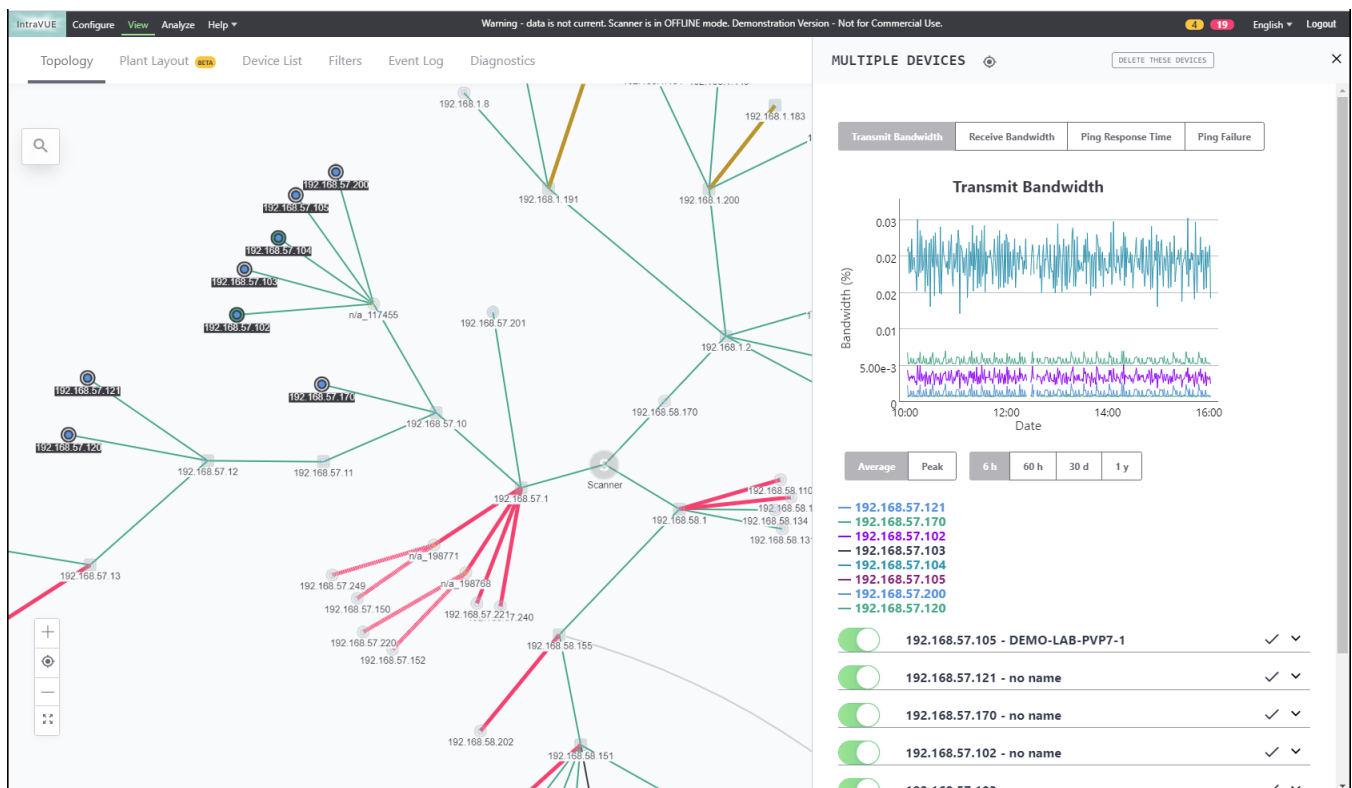
# IntraVUE Architecture

## The IntraVUE™ Architecture:

IntraVUE is a network Visualization, Documentation, Diagnostics, and Analytics platform for current and future needs of IIoT (Industrial IoT), and Industrie 4.0.

Installed as a web server application, IntraVUE helps bridge the gap between end-point devices and any user (IT/OT) by using an internet browser to view remotely the status of any piece of equipment with an IP address.

IntraVUE continuously monitors a device's performance and alerts you about potential end-device problems, provides IIoT and Industrie 4.0 aware users with relevant on-demand network-wide site layout diagrams, and generates self-serve uptime performance Analytics reports about the health of your IIoT, and Industrie 4.0 devices to quickly help you restore productivity and uptime.



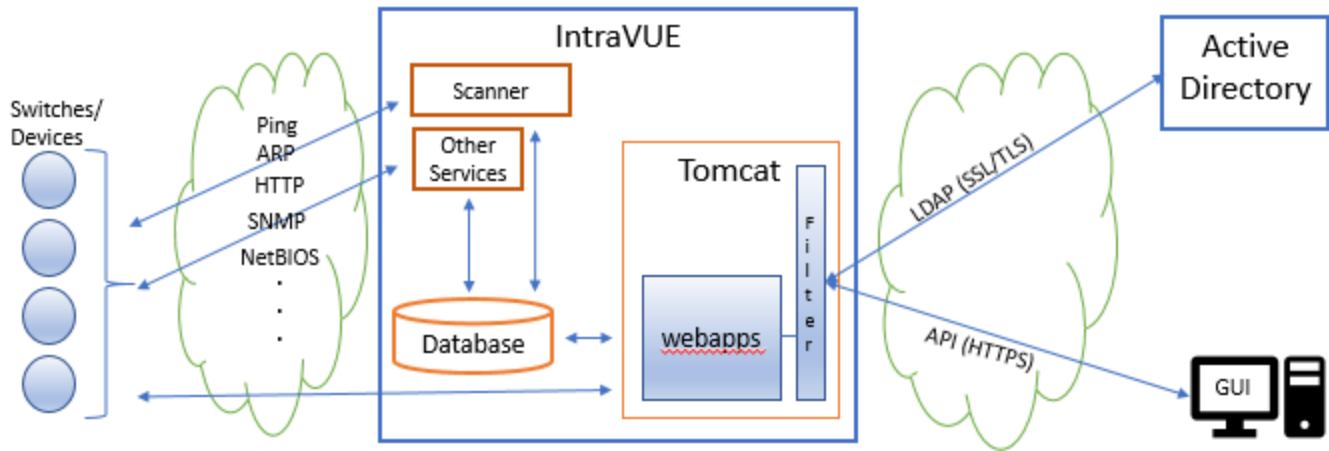
IntraVUE with its new re-designed user interface in HTML 5 continually scans your entire network(s) for new devices, and immediately updates the user interface and event log information when a



device has disconnected, or experiences problems. This dynamic ability is enhanced when IntraVUE Agents are used to visualize remote areas of your IIoT, and Industrie 4.0 infrastructure.

IntraVUE Components:

IntraVUE is made up of several distinct and integrated components:



A simplistic view of the IntraVUE™ server and client (browser).

Server	
Network Scanner	Continuously monitors the configured networks checking for device disconnections, new devices added, and threshold data from SNMP MIB data fields. The scan engine uses Ping and ARP to detect the presence of devices and SNMP to get information about the hierarchy of the network. This information is stored in the database.
Relational Database (Maria DBI)	This is the area in which both scanned information, administrator configurations, and events are stored.

<b>Other Services</b>	<b>Auto-IP</b> <sup>1</sup> Service is an automatic, enhanced <b>BootP</b> <sup>2</sup> server which works in conjunction with IntraVUE. Auto-IP is installed in demo mode if not purchased. KPIs Reports and Dashboards are two additional services.
<b>Web Server (Tomcat)</b>	Provides the framework for hosting and accessing the user interface content.
<b>Client</b>	
<b>User Interface</b>	The browser utilizes a visualization methodology that allows a very complex network to be displayed on a single screen. This visualization is integrated into the user interface and sent to the Client device. The user interface is updated on a periodic basis to allow the most current information to be displayed on any client browser.

---

<sup>1</sup>Automatic Private IP Addressing also known as APIPA or Auto IP is a method of automatically assigning IP addresses to networked computers and printers.

<sup>2</sup>The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951.

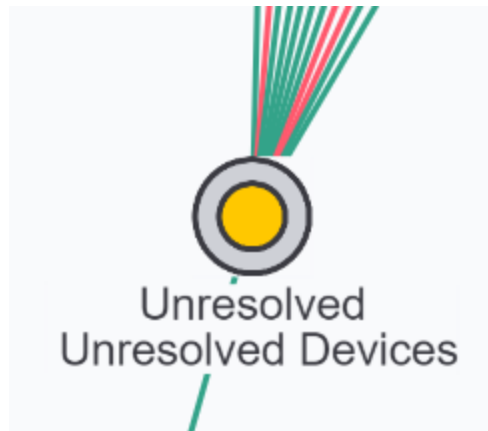
---

# New Installation

1. The first task is to install and register IntraVUE™. See [Installation & Registration](#)
2. Log in as the administrator (see [Adding Users and Changing Admin Password](#)).
3. Go to the Scanner Tab and select Add Network. Select or enter the top parent for your network and then add the IP Address ranges to be scanned. The 'Top Parent' is the device that has the MAC addresses for the devices you want to scan. In most cases this will be the IntraVUE host computer. See [Configure Menu - Scanner Tab](#) for the details of adding a network.
4. Click "Save and Scan" for IntraVUE™ to begin scanning.

When new devices are added the IntraVUE Scanner will spend several minutes developing the Network Topology. Viewing at this time will not provide an accurate depiction of the topology.

Initially IntraVUE will show all discovered devices linked to a special Unresolved node connected to the top parent.

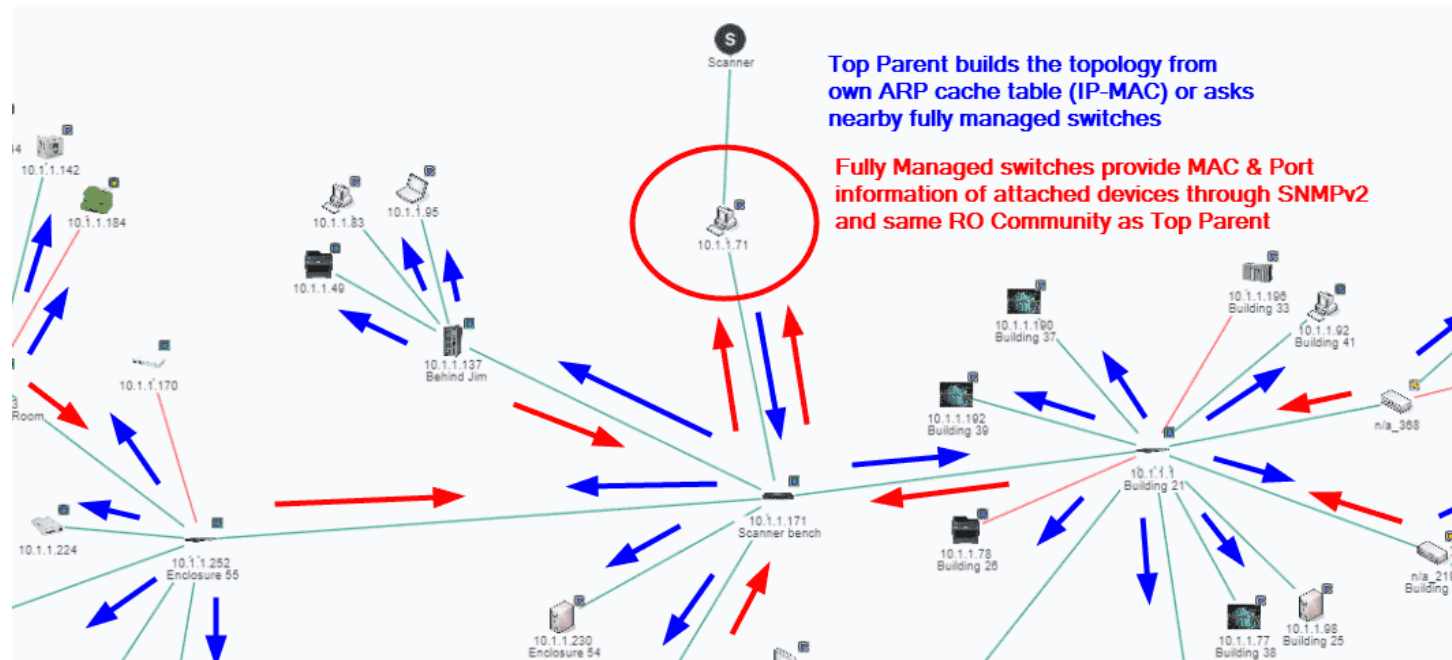


As soon as a device responds to a ping it is placed under the Unresolved Devices node and the individual nodes. During this period IntraVUE first attempts to find MAC address information from the top parent and any local routers or layer 3 switch.



One cause of IntraVUE not determining the MAC address is an incorrect or missing SNMP read-only community setting in a managed router's own configuration, or in the IntraVUE System Configuration Scanner's tab, "Default SNMP Read Only community". This is usually set to 'public'.

Once the MAC address has been determined, IntraVUE attempts to find the correct location in the network hierarchy to place the device.



If the IP of the device is in the same subnet as the top parent it will be moved to the top parent pending a move to a managed switch. If it is in a different subnet from the top parent of that IntraVUE network, it will remain in unresolved unless a router having an interface for that IP is discovered or a managed switch claims its mac address on a port. In those cases the device will move out of unresolved. This situation could occur due to an incorrect community in a router or switch, or its switch is not in the scan range.

Devices under the Unresolved node will have all the functionality of other devices in IntraVUE. The Unresolved node serves as a placeholder for devices that can not be properly placed by IntraVUE with some information indicating the difficulty. See also [Selecting The Top Parent](#).

In the case that switches in a different subnet can not provide MAC information because of lack of access to SNMP on router that bridges the other subnet, you can enable the option "Use SNMP provided MAC" which will provide the MAC address from the SNMP of the switch. See also [Device Configure - SNMP](#).

Accessing SNMP data from the configured routers and managed switches, IntraVUE starts to automatically build the connection information of these devices. This establishes the parent-child relationship. A parent is a device that has other nodes/devices connected to it.

IntraVUE gets hierarchy information by SNMP queries to managed switches. If the community for a managed switch is incorrect or not the default, IntraVUE will be unable to determine the device is managed and the hierarchy will appear to be flat.

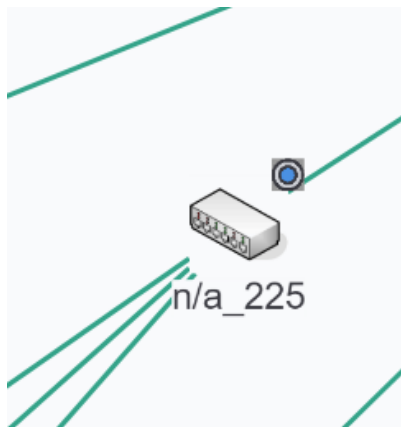
There are, however, cases in which unmanaged switches or hubs have been utilized. If the scan engine discovers two or more devices on the same port of a managed device, the scan engine will assume a hub or unmanaged switch (without IP) is present and automatically insert a node. These nodes will be given a device name of "Auto Inserted Node" and should be edited to describe the actual device.

Provisions in the IntraVUE software have been made for other devices to be manually added and to manually move devices to them. The ability to add and move devices is covered in

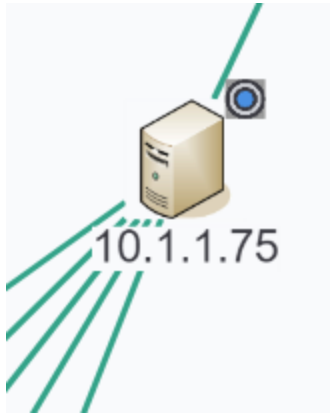
- A good example of this is to add a child to an end node such as a Serial to Ethernet converter, one child for each serial device of the converter..
- Another example is to have a PLC with a serial port connection to a Device server.

This functionality allows the user not only to view the Ethernet device but also the connected device. The PLC would be able to have a device property and even Web Links (via proxy) without the device containing an embedded Ethernet port. To be clear, the actual properties of the PLC would not be viewable; but IntraVUE could be used to show what is connected to the Device Server and information (such as html files) could be associated with the manually inserted device. A field bus to Ethernet device can also be manually inserted in this manner.

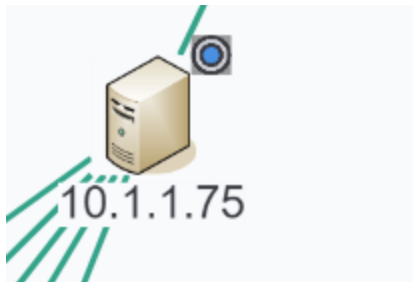
If the read community of a managed switch is not known or is incorrect in its configuration information, IntraVUE will find the switch and place it below an Auto Inserted Node along with all the other devices connected to the managed switch.



When the correct community is set in the device configuration, IntraVUE will move the device to its correct location and move all the devices attached to it to the correct ports of the managed switch.



If the community is unavailable due to security or other reasons, the admin should check the 'unmanaged switch' checkbox in the Device Configuration dialog. IntraVUE will then place any devices seen on the unmanaged port under this device. It will 'look' like a switch but not have any port numbers and will not be able to get snmp bandwidth data for devices without snmp.



- ☐ WAP (CHILDREN ARE WIRELESS)
- ☒ VM, HUB, OR NON-SNMP SWITCH
- ☐ NAT

## Selecting The Top Parent

### What is a **Top Parent**?

Each IntraVUE™ 'network' is a grouping of logical devices depending on the needs of the user. Each IntraVUE™ network consists of a set of scan ranges and a Top Parent.

Only two devices can be a top parent: the host computer and a router (layer 3 switch) for which the snmp community is known.

### Definitions:

The **Top Parent** of an IntraVUE™ network is the device which can provide the MAC addresses for the devices in the scan range.

**Local:** all devices in the same subnet as the IntraVUE™ host ip address.

Local is determined by applying the IP address of a computer to its subnet mask. Pings to local ip addresses will go directly to the device and the MAC will be stored in the host computer's ARP cache.

An online subnet calculator is useful if you have unusual subnet masks. [www.subnetonline.com](http://www.subnetonline.com) and [www.subnetmask.info](http://www.subnetmask.info) are two examples.

**Remote:** all devices NOT in the same subnet as the IntraVUE™ host ip address. Pings and other traffic to remote devices will leave the local subnet and go to the default gateway (a router) if one is configured. The gateway will use its routing tables to direct the traffic to one of its interfaces or its gateway if it does not have an appropriate interface.

General rules for determining the 'top parent':

The IntraVUE™ host computer must be the top parent if any devices in an IntraVUE™ network are local to the host. This is because the MAC addresses will be in the host's ARP cache as a result of the scanner's pings.

The MAC addresses for any devices not 'local' to the IntraVUE™ host computer will be in a router. They will be in the last router leading to a device, the so-called 'last hop router'. **Generally, the gateway IP address of a remote subnet is the correct top parent for that subnet.**

A router only needs to be in one IntraVUE™ network to find the MAC addresses for all other IntraVUE™ networks. Putting the router in its own IntraVUE™ network with no other devices is one method of doing this.

The IP address of a network's top parent must be included in one of the IP address ranges for that network.

*Again, the top parent of each IntraVUE™ network is the device which has access to the MAC address information on the devices that will be in its scan range(s).*

A very detailed document covering the configuration of many types of networks, from very simple to very complex is at [How To Configure IntraVUE™ networks](#)

The scanner will attempt to identify any routers that are in a scan range and the scanner will try to get additional MAC addresses from any router it finds.

If an IntraVUE™ network has some devices that are local and some devices that are remote, the host computer must be the top parent and one (and only one) of the router's ip addresses should be in a scan range.

If you have VLAN's each VLAN should be in a separate IntraVUE™ network. This will result in clearly showing the path traffic takes to go from one device to another.

If switches are in a separate VLAN, that IP address range can be added to each other VLAN's scan ranges. Thus, each IntraVUE™ network will have the switches and show how devices are connected. Switches that are not used in a particular VLAN can later be deleted from that IntraVUE™ network.

**Example:**

If there is one router and many VLANS and you want to scan those VLANs, make the interface (IP) of the router of that VLAN the top parent for that VLAN. This will make it easier to navigate the browser when there are many VLANs or networks.

IntraVUE™ host is 10.1.1.35.

*Router has IP addresses 10.1.1.1, 10.1.2.1, 10.1.3.1, and 192.168.1.254.*

*You want to scan all those class C ranges.*

**Network 1**

*top parent 10.1.1.35 (local host to get MACs of local devices)*

*range 10.1.1.0 - 10.1.1.255 (includes the router 10.1.1.1 and top parent)*

**Network 2**



*top parent 10.1.2.1*

*range 10.1.2.1 - 10.1.2.255*

*Network 3*

*top parent 10.1.3.1*

*range 10.1.3.1 - 10.1.3.255*

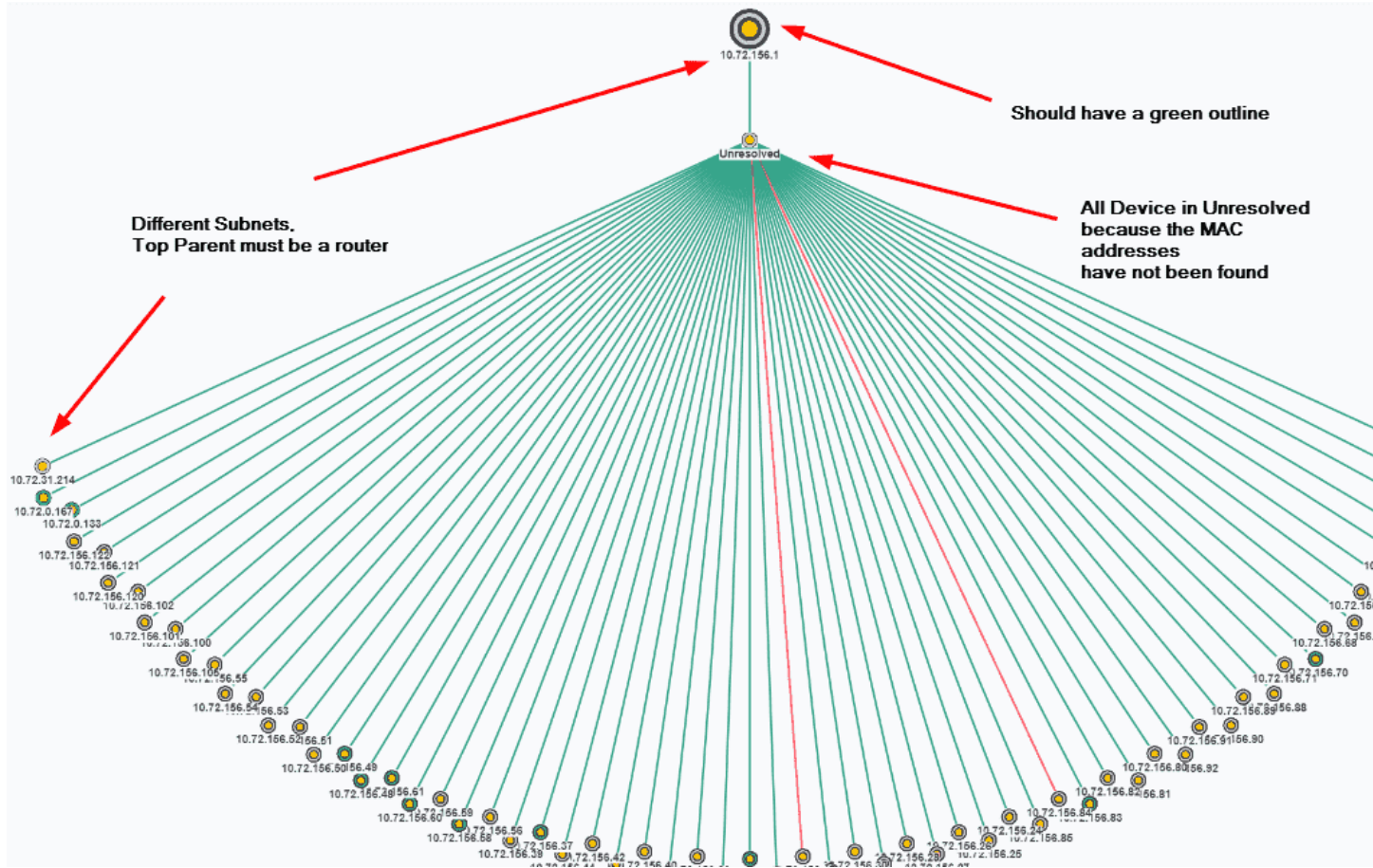
*Network 4*

*top parent 192.168.1.254*

*range 192.168.1.1 - 192.168.1.254*

IF YOU ARE SCANNING ANY DEVICES LOCAL TO THE HOST COMPUTER, the host is the ONLY device which can be the top parent. This is because only the host will have the MAC addresses for the local devices which the scanner is pinging. (While the gateway router may know some of the MACs it will only know the ones that communicate outside the local subnet.

### **Unresolved Nodes Problems**



If you do not select the correct top parent, or the top parent is not configured to successfully use SNMP, you will see something like the image below in your browser.

If the top parent is not the local computer, it must be a router because routers are devices that tell mac addresses when provided an IP address. In the image, the top parent is in an IP address range separate from the devices that are scanned. That is a clue that the top parent must be a router.

In the image, there is no green outline surrounding the top parent node. If the IP of the top parent IS a router, then the SNMP community is not correct or the router has been configured with an Access Control List and the IntraVUE™ host is not on the list.

If the top parent is not the local computer, it must have a green outline indicating there is successful SNMP communication with the ROUTER that knows the MAC addresses of the devices in the scan range.

See also [Configure Menu - Scanner Tab](#), and [Completing Initial Configuration](#).

## Installation & Setup

## User Functions

## Accessing IntraVUE™ remotely via any Internet Browser

IntraVUE™ is designed to scan locally and be viewed remotely. The user interface is all through a browser. There is no expectation that you need to have physical access to the computer hosting it.

In order to browse to IntraVUE™ you need to know an ip address or URL of the computer hosting it.

Most HTML 5 compatible browsers must start the address with "http://", then append the ip address, then add ":8765".

Examples might look like "http://192.168.10.15:8765" or "http://nameOfComputer:8765"

The 8765 is the non-standard browser port used by IntraVUE™ to avoid conflict with Microsoft IIS or other possible web servers typically hosted on port 80 or 8080.

If you can ping the IntraVUE™ host computer's ip address remotely, you can browse to IntraVUE™.

If you can't ping the IntraVUE™ host remotely you may need to open a VPN connection to the host.

If you can ping the IntraVUE™ host but the page is not found, perhaps port 8765 is being blocked by a firewall or network security setting somewhere in between the connection or in the actual IntraVUE™ host itself.

## First Login

There are only two types of user types in IntraVUE - Basic USER and ADMIN.

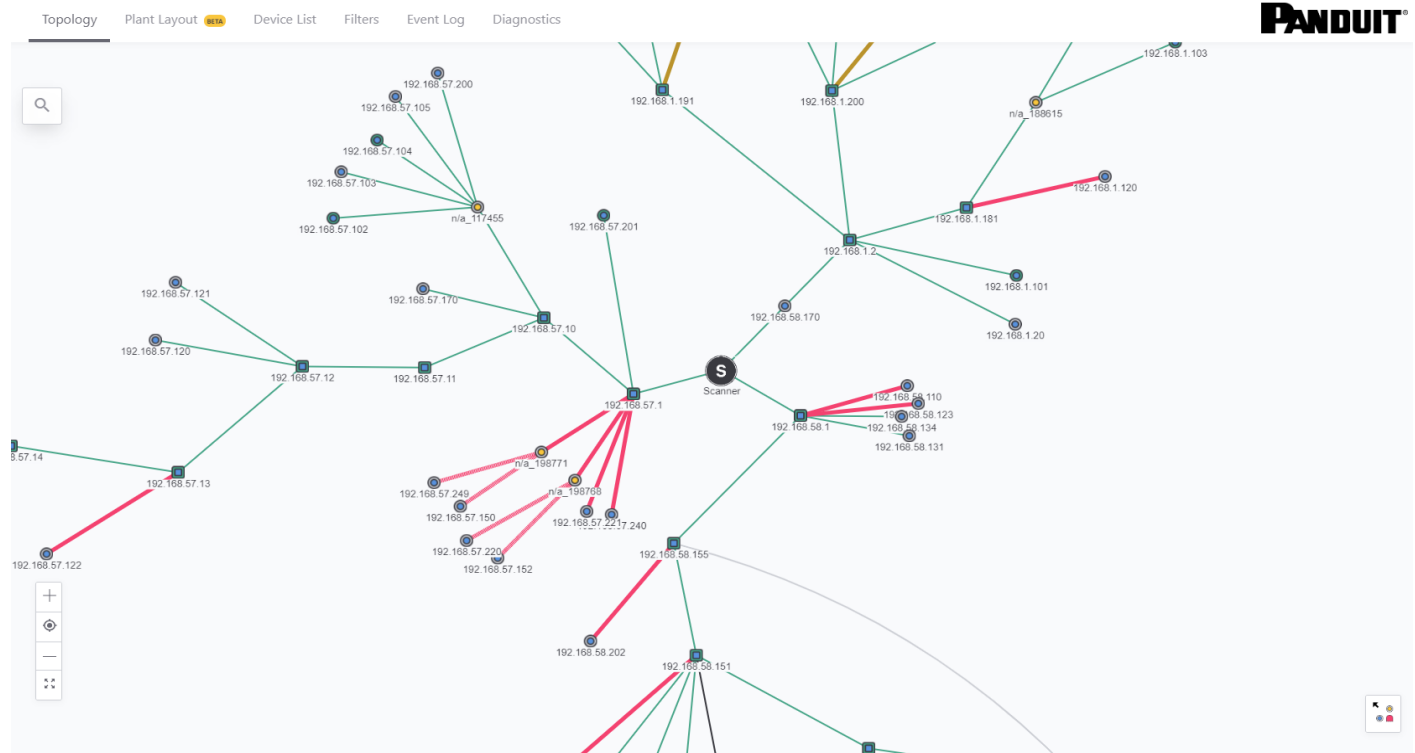
A Basic USER sees the default view to all the data that is available without having to log in into IntraVUE™.

The ADMIN user configures IntraVUE in the Configuration menu and Device Side View Edit mode.

In order to have ADMIN privileges a user must login as user 'admin' and password 'intravue', or have a username with admin role and enter a password.

You may configure Tomcat to require a different user name and passwords in order to access the IntraVUE web page, see [Adding Users and Changing Admin Password](#)

## Topology View



The initial browser view of IntraVUE shows the organization of all devices within each configured network. This is called the **Topology view**.

The IntraVUE™ 3 user interface is provided thru a browser such as Internet Explorer or Mozilla Firefox. On the host computer the URL can always be entered as `http://127.0.0.1:8765`. From any other computer that can ping the host, you may see the same thing by substituting the IP address of the host for the 127.0.0.1, for example `http://192.168.1.55:8765`. Note: the colon and 8765 is required after the IP address and typically you must also enter the `http://` in Internet Explorer.

A [video](#) is available which covers basic navigation, colors, and operation IntraVUE™ 3.

The Top Parent of each network will be one node away from the "scanner" node at the center of the screen. The network is visualized as a star or tree of devices radiating out from the "scanner". This patented method is called a hyperbolic tree.

Individual devices or nodes are shown as colored circles connected by colored lines indicating the connection between the devices.

Drag all nodes on the screen by holding down the left mouse button until the part of the network you are interested in get toward the middle. Attributes of nodes are largest in the middle when you zoom in and they gradually disappear as you zoom out or move in either direction (north, south, east, and west).

You can think of the IntraVUE visual display as a flat network diagram that has been wrapped around a ball, and you can see only part of the ball.

This graphical feature allows very complex networks to be displayed in a single window.

## **View Controls**

There are several controls that may be used with the IntraVUE user interface.

- **DEVICE** - click on a device brings up a right slider bar with Single View Details including Device Info (Default Details, Advanced Details), Threshold Graph, Events Log.
- **SWITCH** - click on a switch or router brings up a right slider bar with Single View Details (Device Info, Threshold Graph, Events Log), and Sideview Aggregate Details (Multi-Device Threshold Graphs).
- **ROUTER MENU** - click on a device brings up a right slider bar with Single View Details including Device Info (Default Details, Advanced Details, Additional Interfaces), Threshold Graph, Events Log.
- **CONNECTION MENU** - click on a connection line to bring up information about the connecting nodes including Port Information, Ping Response/Failure Graph, and Transmit/Receive Bandwidth Graph.
- **CRTL-KEY LEFT CLICK HOLD MOUSE BUTTON** - to draw an area around multiple nodes to bring up the Threshold graphs just for these highlighted devices.
- **DRAG WITH LEFT CLICK HOLD MOUSE BUTTON** - moves the entire network to shift the devices that are seen in the center or edge of the browser page.
- **ALT-KEY PLUS LEFT MOUSE BUTTON** - shows the line length factor as a black circle. If you continue to hold the mouse button down you may change the size of the line length. This is applied to all lines.
- **HIDE SLIDER** - click on the map view to clear right side slider bar.



- **MULTIPLE DEVICES** - CTRL-KEY LEFT CLICK HOLD MOUSE BUTTON DRAG AREA - opens a slider on the right side showing IP addresses of the highlighted devices.

### Admin Controls

This is another form of the Mouse Controls above. Requires you to login as Admin.

- **SYSTEM MENU** - click on the header bar options (Configure, View, Analyze, Help, About, Login, Topology, Plant Layout, Network List).

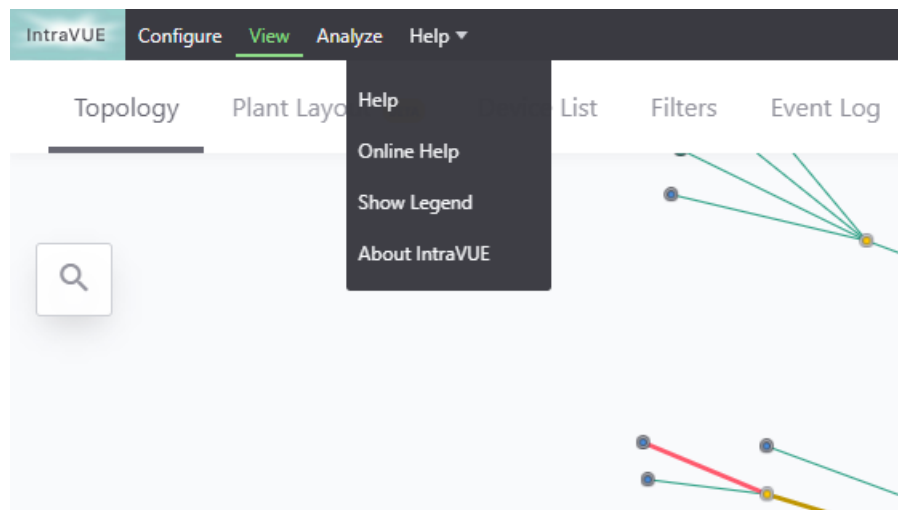
- **DEVICE MENU** - right slider panel with options for device, switch, router, connection,



Network List allows you to display in both Topology and Plant Layout views a subset of configured networks by using the toggle button for each network.

- **EXTRA INTERFACE INFORMATION** - zoom in or zoom out to see the other IPs of devices like routers.

### Help



Under the Help drop-down, there are four options.

- » **Help/Online Help**- This options brings up the latest version of the IntraVUE Online Help System.
- » **Show Legend** - This enables the node legend at the bottom-right corner of the screen.

- » About IntraVUE - The Version number and expiration date of the IntraVUE service contract can be viewed here.

## Sub-Levels View

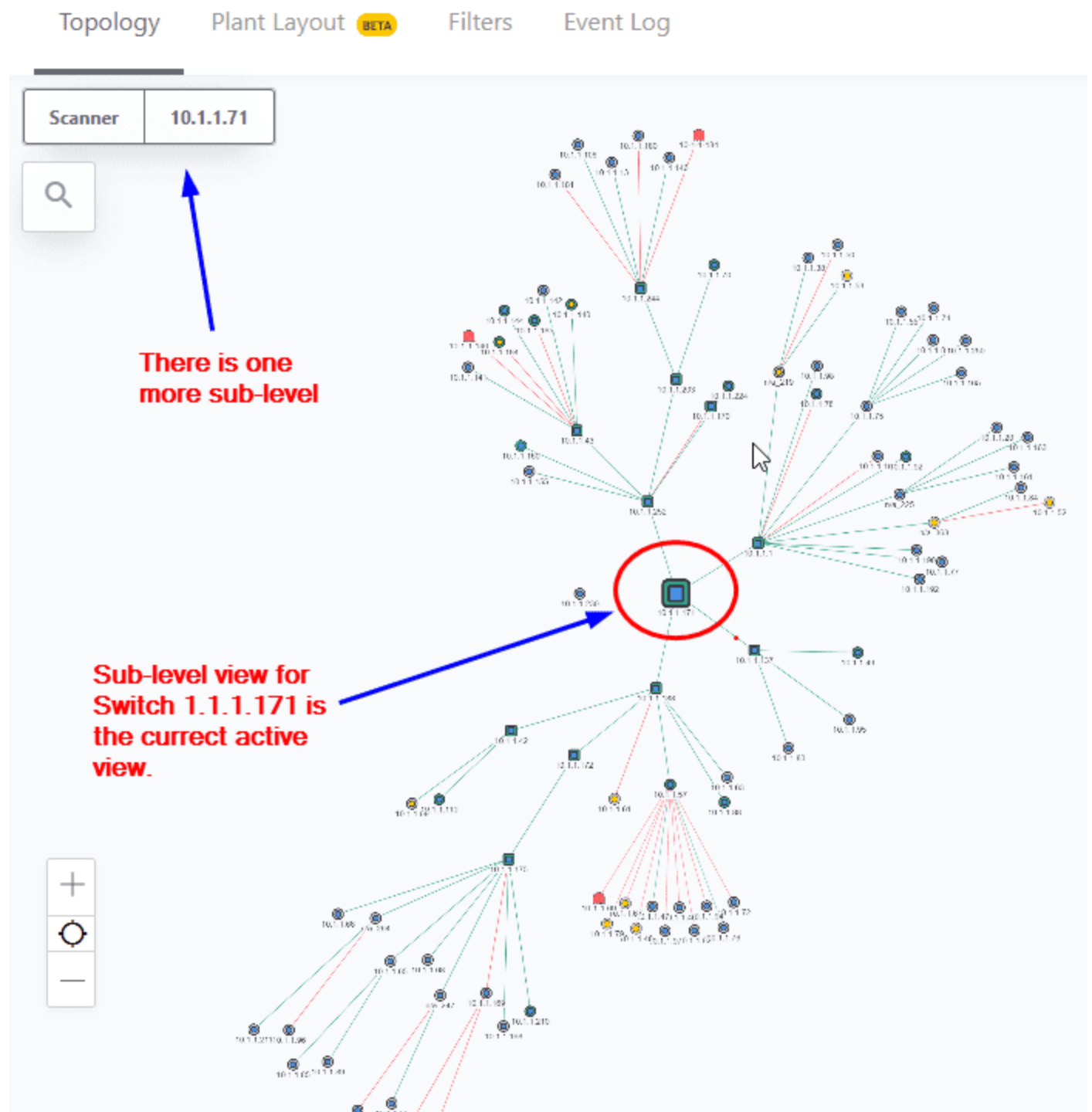


To simplify the view of a complex network, nodes or switches that have child nodes connected to them may be hard to see as the number of nodes in the topology view increases.





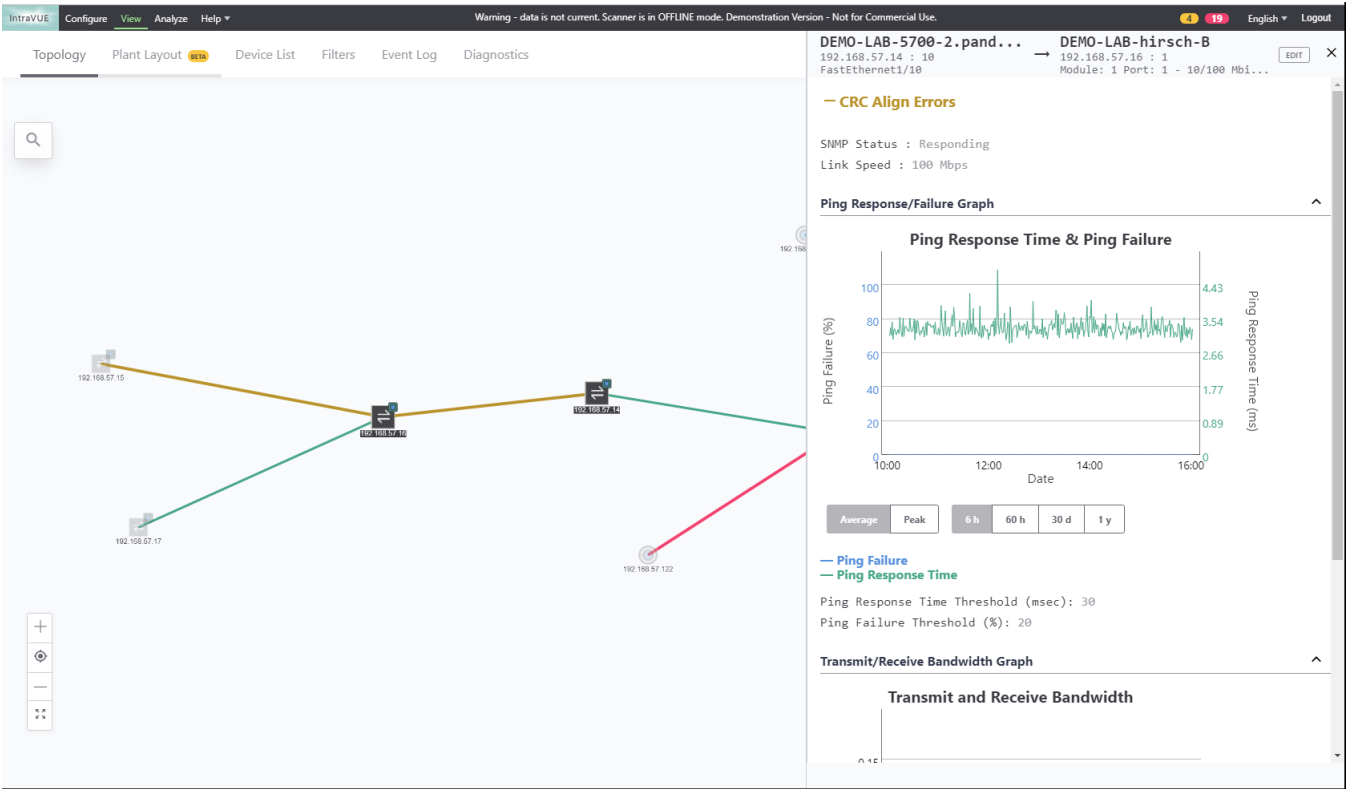
To go up one or more levels in the sub-level views simply click on one of the parent switches IP addresses. If you want to go back to the Scanner Level view simply click "Scanner".



This view does not prevent any alarm or threshold event from occurring.

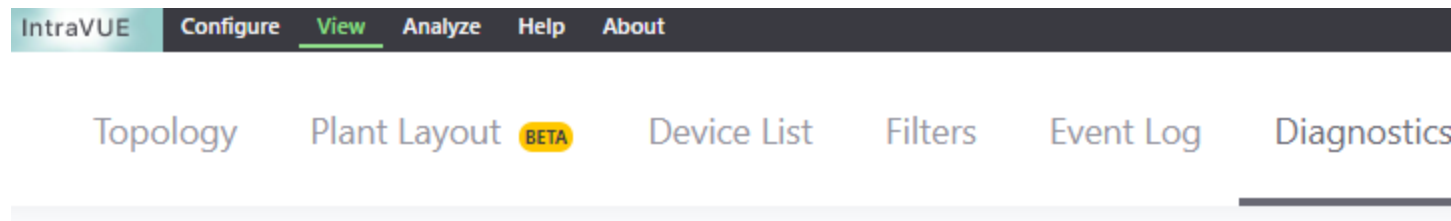
Alternatively, you can also make IntraVUE™ only show one or a combination of configured IntraVUE™ networks. See [View Filters](#)

CRC in Topology View



Upon clicking connecting lines, this displays a sideview of CRC and IfInError data.

# Navigation Menu



The System Menu contains two 'sections'.

The first section contains the navigation options.

**Configure:** Admin settings

**View:** Visualization Home

**Analyze:** Standard KPIs Analytics Dashboard

**Help:** Contains the IntraVUE™ Help (Starting Guide, Advanced Guide, Tutorials, FAQs, Known Issues, Tools)

**Login** allows you to log on to IntraVUE™ from any browser

**Logout** allows the to log out of IntraVUE™

The second section contains views related to auto-discovery

**Topology View:** This is the main view. See [Topology View](#)

**Plant Layout View:** Alternate view that can be modified according to your plant map. See [Creating Plant Documentation](#)

**Filters View:** Both Topology View and Plant Layout View can be filtered according to one of these filters. See [View Filters](#)

**Event Log View:** This view allows the user to access all activity for all devices. See [Event Logging](#)

**Device List:** This view allows you to see CRC errors for devices. See [Diagnostics View](#)

**About** contains version number, service contract expiration, and third-party notices

## Multi-Language Support



IntraVUE™ supports the following languages when you click on the drop down. All text label will appear in the language of choice (except the Event Log entries).

**English**

**Spanish**

**Chinese**

**French**

**Japanese**

**German**



# IntraVUE Legend

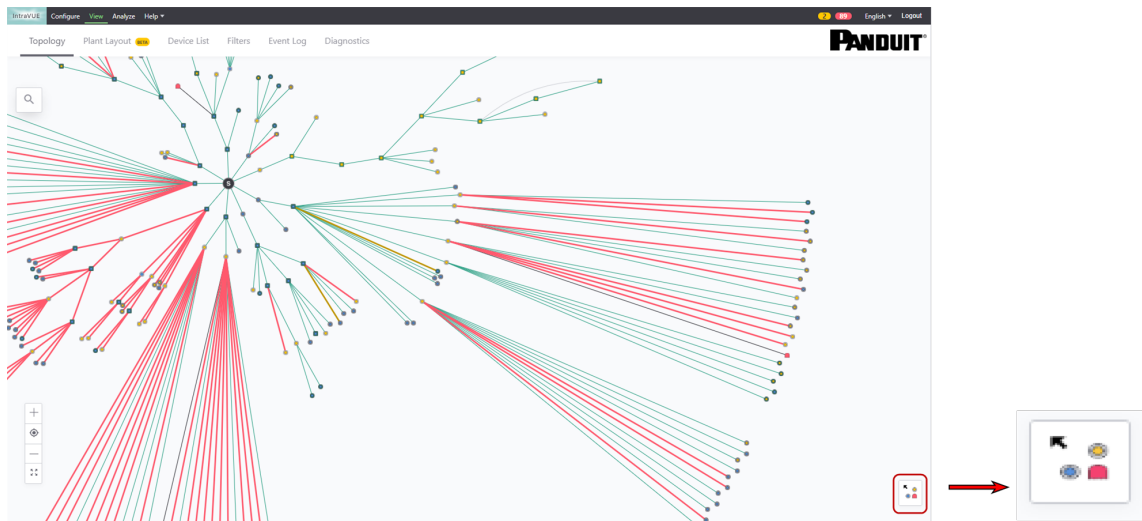
IntraVUE™ makes extensive use of colors. In addition to this [help page](#), a video showing Use of Colors is available.

A node represents a device and is a circle in the IntraVUE™ display. The node may have one of 3 fill colors and one of 4 outline colors.

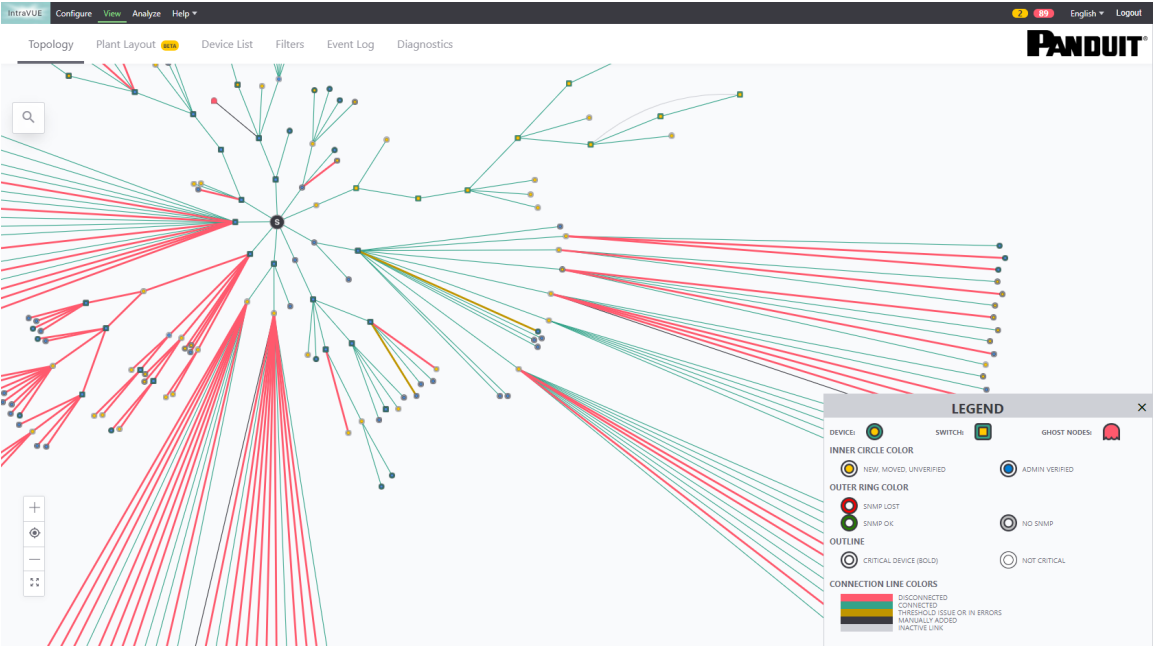
-----

The Color Legend in the bottom-right screen can be enabled or disabled in Topology View and Plant Layout View.

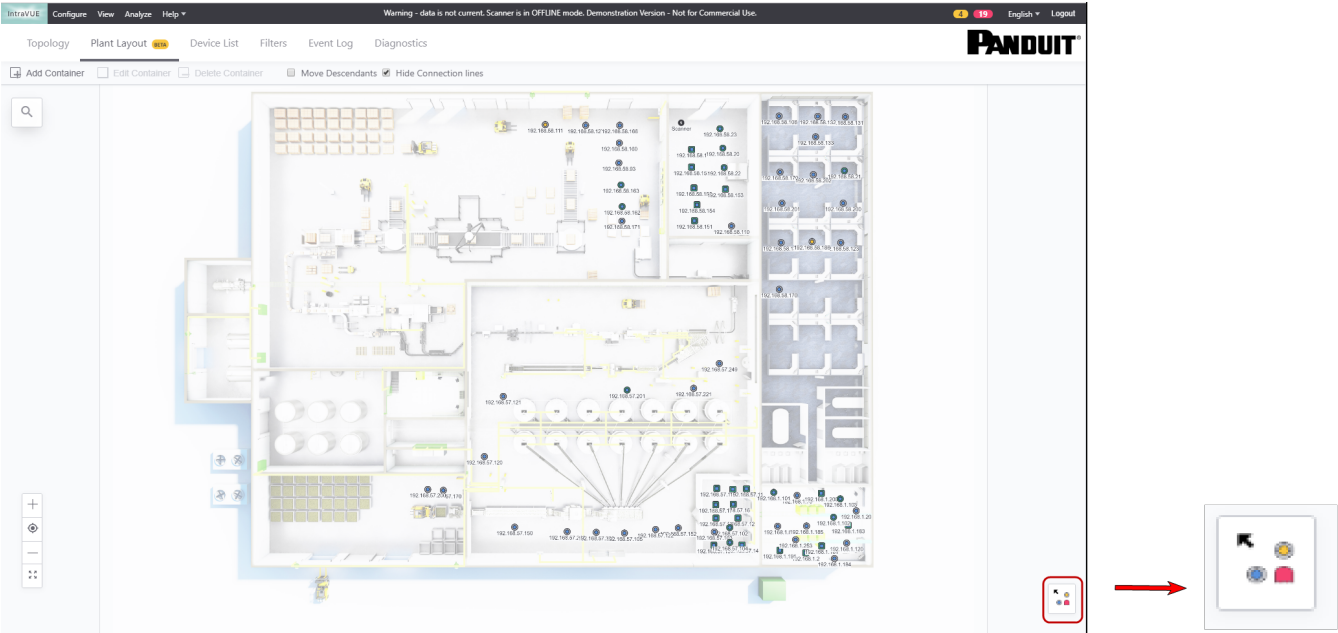
## Disabled Legend

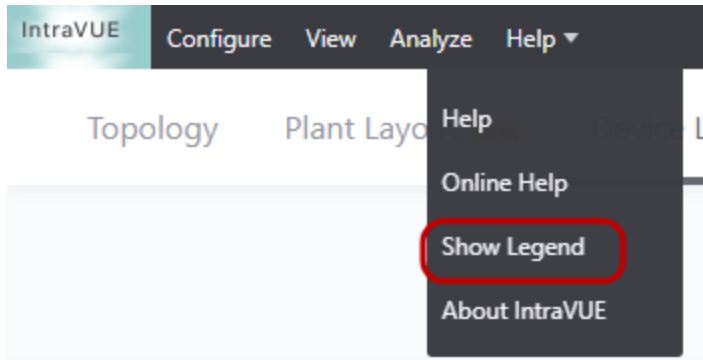


## Enabled Legend



Plant View Legend





There is an option in the Plant Layout View that displays the Legend.

1. Hover over the **Help** drop-down menu.
2. Select **Show Legend**.
3. The color legend will expand in the bottom-right corner.

### NODE FILL COLORS



Newly discovered device that has not been verified by the administrator appear in a light-brown color.

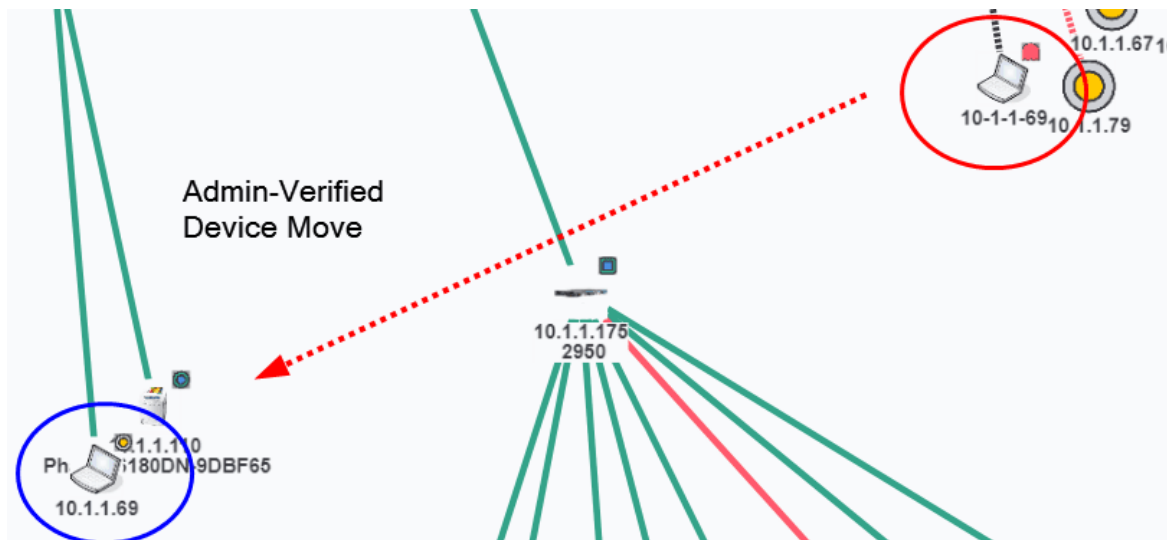


Newly discovered device verified by the administrator appear in a blue color.



Admin-verified ghost node.

Once a device has been verified by the administrator the node will be blue. A normal network should have all the device nodes in blue. If a new device joins the network it will be easy to spot the light-brown box. See [Admin Verification in IntraVUE 3](#) for more details.



If an Admin-Verified device moves, the verified position will be represented by a red-filled ghost image. At the new location, a new, unverified node will be placed representing the actual location of a device. See for more details.

## NODE OUTLINE COLORS



A device which currently has SNMP communication with IntraVUE™ has a green outline.



A device which currently has SNMP communication with IntraVUE™ has a green outline. Critical Status enabled device.



A switch device which currently has SNMP communication with IntraVUE™ has a green outline. Admin Verified.



A switch device which currently has SNMP communication with IntraVUE™ has a green outline. Critical Status enabled and Admin Verified device.

**NOTE:** if a device is disconnected and there is a red line to the device, there may still be a green outline as the scanner does not test SNMP on disconnected devices, nor does it create SNMP lost/-gained events for disconnected devices.



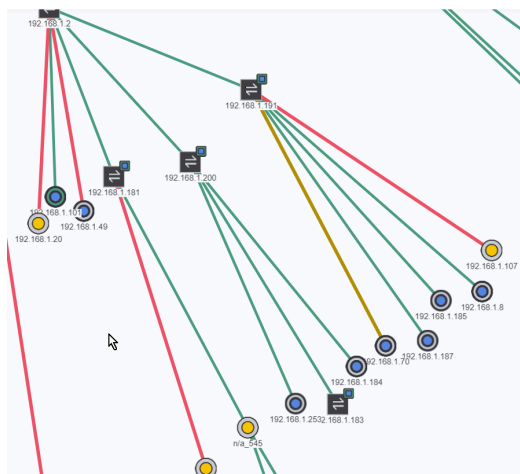
If the last 2 SNMP queries timed out, the event will be logged and the device will get a red outline until SNMP is regained.



If the last 2 SNMP queries timed out, the event will be logged and the device will get a red outline until SNMP is regained. Critical status enabled.

---

### CONNECTING LINE COLORS



Five line colors are supported in IntraVUE™.

- » GREEN - indicates a device is currently connected and capable of communicating.
- » YELLOW - indicates one of the threshold factors for this line is over the threshold condition. If a device has current CRC or IfInErrors, the lines will also be yellow.
- » RED - means the device is currently disconnected and not responding to pings.
- » BLACK - is used when you manually insert a node and there are no pingable devices below it.
- » BLUE - means the line is selected by a left-click.

**NOTE:** When zoomed out, YELLOW and RED lines are bold.

A **dashed** lined instead of a **solid** line indicates that the device is a wireless device.

# Search Devices

Search provides a quick way to find devices when there are a large number being displayed.

IntraVUE

ConfigureViewAnalyseHelpAbout

Warning - data is not current. Scanner is OFFLINE

TopologyPlant LayoutBLTAFiltersEvent Log

×

View Details

IP Address	Device Name	MAC Address
10.1.1.71	MARK-PC	60 EB
10.1.1.171	Dell Managed Switch	00 11
10.1.1.137	Ethernet Direct Managed Switch	00 18
10.1.1.49	Printer	00 1B
10.1.1.95	CDOYLE-HP	88 51
10.1.1.83	CLAIRE-DESKTOP	00 11
10.1.1.188	N-TRON Managed Switch	00 07
10.1.1.63	Dell Managed Switch	78 2B
10.1.1.88	SUZANNE-PC	00 1A
10.1.1.57	Dell Wireless Router	00 C0
10.1.1.72	OP-JSAH-MACBOOK	28 5A
10.1.1.76	BILL-MACBOOK	8C 58
10.1.1.94	JESSE-LAPTOP	84 3A
10.1.1.62	Scanner 25	88 32
10.1.1.46	Scanner 26	F8 F1

You can find devices by IP address, device name, network name, or by MAC.

When you change the text on the search box, the results change to remind you of your selection.

Below is the name search.

Regardless of which type of search you use, the search is automatically prefixed with a wild card.

This means that a match will be found for everything that contains any number of characters before the text you entered as search criteria.

For IP addresses there are several options.

- » You may enter the full IP address and only that one IP will be found.
- » You may enter a number without any periods to find the IP having that number as the last octet. For example, a "1" will find X.X.X.1, X.X.X.21, and X.X.X.151.
- » You may enter a single period followed by a number and only the IPs having that number will be found. For example, a ".1" will be find X.X.X.1 but not X.X.X.21.
- » Any other combination will find that literal text combination. For example, a ".100." will find all X.100.X.X's, X.X.100.X's, but not X.X.X.100.

For MAC addresses, the hexadecimal MAC address to be found must be entered in pairs. The hex pairs may be separated by spaces, colons, or periods.

The sample dialog above shows that 16 devices have a "1" in their last octet. We are looking at the 4th match.

The search dialog is updated for each found device's View Names as well as its MAC address.

There are two explicit wild card characters you could use in searches, '\*' and '?'.

- » A '\*' will match any number of any characters.
- » A '?' will match only one character. So '.11?' will match .111, and .114, but not .11.

You may use the **Prev** and **Next** buttons to go through the list of found devices and each selection will center that device in the browser.

ur own content.



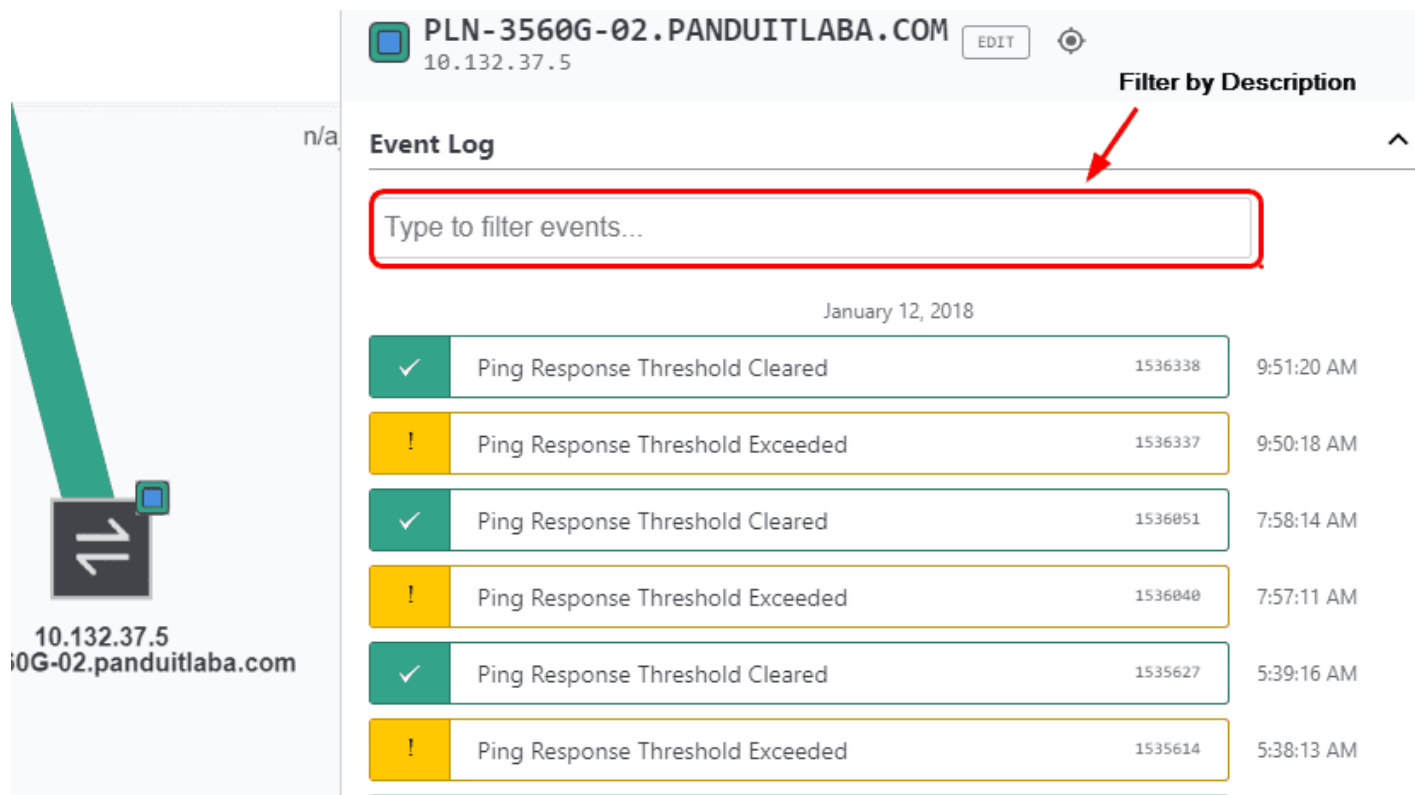
## Event Logging

IntraVUE™ continuously monitors all activity on the network. To access the events for a single device, the Side View for that device contains its own events. To access the details of the entire network, click **Event Log** from the Navigation menu.

### Device Event Log

The initial Device Menu Side View contains a device's Event Log which maximizes screen space to display a particular device's history of events in descending order by date, but which also show by critical colors, IP Address, description, and date time stamp for every event.

You can search for the event log on this device for specific event log descriptions (e.g. disconnected, ping response, etc).



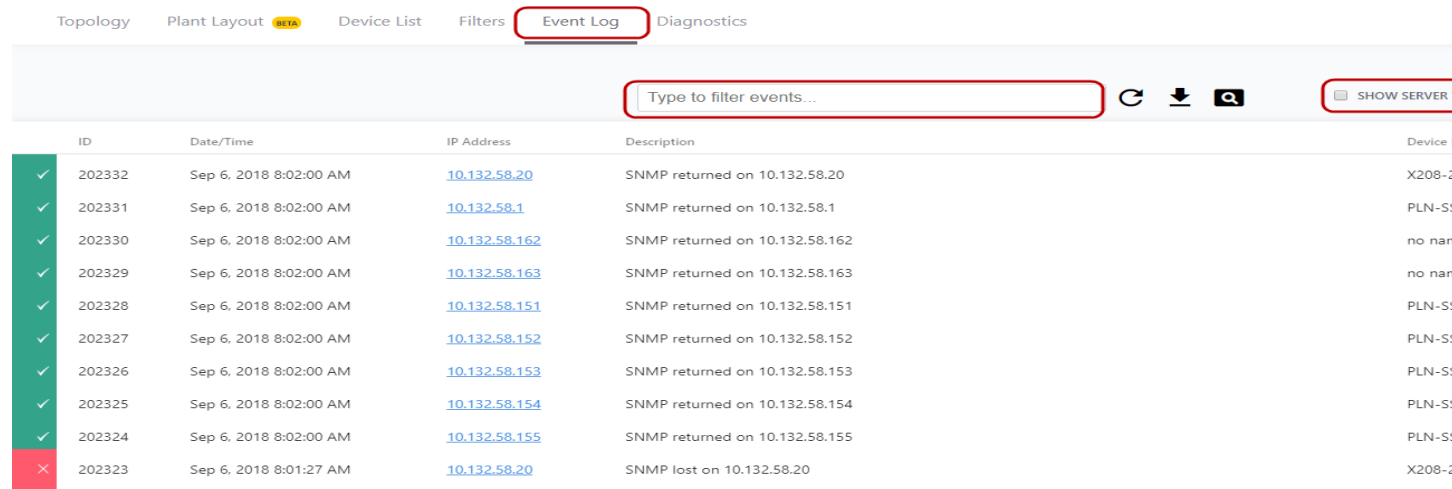
The screenshot displays the IntraVUE interface for a specific device. On the left, a device icon is shown with the IP address 10.132.37.5 and the name i0G-02.panduitlaba.com. The main panel shows the Event Log for device PLN-3560G-02. The header includes the device name, IP address, an EDIT button, and a Filter by Description dropdown. A search bar with the placeholder text 'Type to filter events...' is highlighted with a red box. Below the search bar, the date 'January 12, 2018' is displayed. The event log contains a list of events, each with a status icon (green checkmark for 'Cleared' and yellow exclamation mark for 'Exceeded'), a description, an ID, and a timestamp.

Status	Description	ID	Timestamp
✓	Ping Response Threshold Cleared	1536338	9:51:20 AM
!	Ping Response Threshold Exceeded	1536337	9:50:18 AM
✓	Ping Response Threshold Cleared	1536051	7:58:14 AM
!	Ping Response Threshold Exceeded	1536040	7:57:11 AM
✓	Ping Response Threshold Cleared	1535627	5:39:16 AM
!	Ping Response Threshold Exceeded	1535614	5:38:13 AM

**Note:** there is only one Side View dialog. Once opened you can switch between all devices and just the ones you want to view click each device. The event log for each device will be updated as you click on each device separately.

## Global Event Log

The global Event Log view contains event for all devices. When the event log is initially launched, it defaults to the full view and no filters are set.



ID	Date/Time	IP Address	Description	Device
✓ 202332	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.20</a>	SNMP returned on 10.132.58.20	X208-2
✓ 202331	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.1</a>	SNMP returned on 10.132.58.1	PLN-S
✓ 202330	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.162</a>	SNMP returned on 10.132.58.162	no nam
✓ 202329	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.163</a>	SNMP returned on 10.132.58.163	no nam
✓ 202328	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.151</a>	SNMP returned on 10.132.58.151	PLN-S
✓ 202327	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.152</a>	SNMP returned on 10.132.58.152	PLN-S
✓ 202326	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.153</a>	SNMP returned on 10.132.58.153	PLN-S
✓ 202325	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.154</a>	SNMP returned on 10.132.58.154	PLN-S
✓ 202324	Sep 6, 2018 8:02:00 AM	<a href="#">10.132.58.155</a>	SNMP returned on 10.132.58.155	PLN-S
✗ 202323	Sep 6, 2018 8:01:27 AM	<a href="#">10.132.58.20</a>	SNMP lost on 10.132.58.20	X208-2



Selecting the IP address of a device will center that device in the Topology View.

In the full view you can filter events by clicking each of the column buttons or you can use the search for specific events based on the following criteria.

- » Event Description (or Type)
- » Network - if more than one IntraVUE™ network is defined, you can view events for all IPs or only the IPs in selected networks.
- » IP Addresses can be ordered in IP address order or in Device Name order
- » Select if results should start with the first or last event, an event number, or at a particular date and time. (Click once or Twice on column name for Ascending or Descending order)
- » Define text which must be in the event description
- » The Show Server Time check box is available

When filtering by IP address, only the highlighted IPs will be displayed.

Once data is entered into the event log it is permanent. IntraVUE™ fetches event log data from the IntraVUE™ server. Information will be available for any device ever scanned by IntraVUE™, even if the device is no longer available.

**NOTE:** if an IP address is re-assigned because the device has been deleted, the new instance will be a different device in IntraVUE™.

You can download the filtered and unfiltered Event Log by clicking the downward arrow.

In order to keep the overall size of the IntraVUE™ database reasonable, old events are periodically removed when they exceed certain limits. The limits are on a device by device basis. These limits are set in the `ivserver.properties` file.

The default limit for events considered of lower importance is 50. Once the limit is exceeded, 50 events will remain but all the ones that exceed the limit will be replaced by a note in the oldest kept event '(previous similar events discarded)'.

- » Events in this low importance group are:
- » Ping Response exceeded/cleared.
- » Bandwidth Threshold exceeded/cleared.
- » connection/disconnection
- » device moves
- » snmp lost/returned
- » Traps: In addition to recording events detected by the IntraVUE scanner in the Event Log, any trap messages that are received by the IntraVUE host will be added to the Event Log. The scanner will listen to the traps port and record all traps that are received, regardless of the sending IP address. Traps can quickly fill or obscure other events in the Event Log therefore we advise only sending traps to the IntraVUE host IP when there is a strong need.
- » name changes

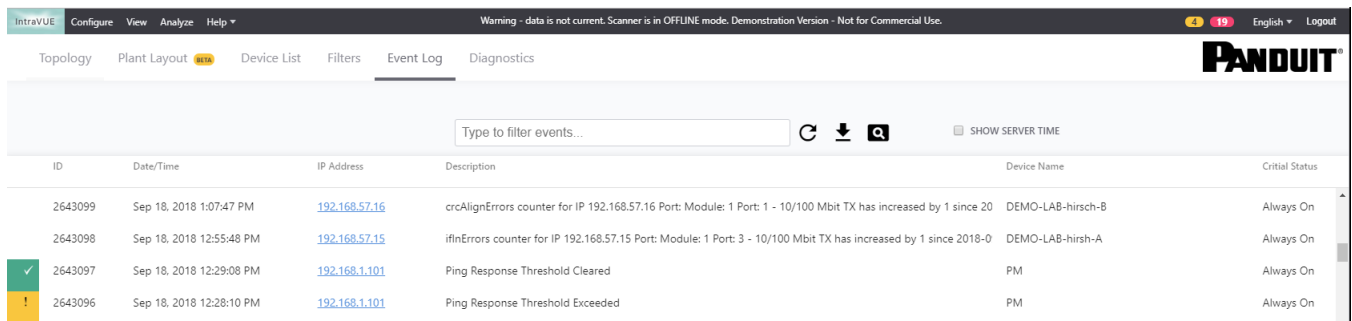
All other events are similarly removed except the default limit is 200 events. Events in this group include:

- » Devices join network
- » snmp supported

- » admin verification
- » changes in ip or mac
- » deletions
- » scanner stopped
- » added child node

See [Event Log Descriptions](#) to learn more about each Event Log description

## Event Log for CRC Data



ID	Date/Time	IP Address	Description	Device Name	Critical Status
2643099	Sep 18, 2018 1:07:47 PM	<a href="#">192.168.57.16</a>	crcAlignErrors counter for IP 192.168.57.16 Port: Module: 1 Port: 1 - 10/100 Mbit TX has increased by 1 since 20	DEMO-LAB-hirsch-B	Always On
2643098	Sep 18, 2018 12:55:48 PM	<a href="#">192.168.57.15</a>	iflnErrors counter for IP 192.168.57.15 Port: Module: 1 Port: 3 - 10/100 Mbit TX has increased by 1 since 2018-0	DEMO-LAB-hirsh-A	Always On
✓ 2643097	Sep 18, 2018 12:29:08 PM	<a href="#">192.168.1.101</a>	Ping Response Threshold Cleared	PM	Always On
! 2643096	Sep 18, 2018 12:28:10 PM	<a href="#">192.168.1.101</a>	Ping Response Threshold Exceeded	PM	Always On

The Event Log under filters data for CRC and IFLN error events. Selecting the Filter options allows more filtering options when configuring data by IP address, Date/Time, and Device Name. See for further information.

## Event Type Filter

Under **Event Log**, select the filter option to display available filters.

1. Choose a Filter and press **Apply**.

The screenshot shows the IntraVUE Event Log interface. The top navigation bar includes 'IntraVUE', 'Configure', 'View', 'Analyze', and 'Help'. The main menu has 'Topology', 'Plant Layout', 'Device List', 'Filters', 'Event Log', and 'Diagnostics'. The 'Event Log' tab is active, displaying a table of events. A search bar at the top of the table says 'Type to filter events...'. A red box highlights the 'Event Type Filter' dialog box, which is open on the right side of the screen. The dialog box has a title bar with a search icon and a 'SHOW SERVER TIME' checkbox. It contains two sections: 'Event Type Filter' and 'Selection Criteria'. The 'Event Type Filter' section has several toggle switches for 'Admin', 'Scanner', 'Moves', 'Mac/IP change', 'Bandwidth', 'Ping', 'Connection', 'IN/CRC Error', and 'Other'. The 'Selection Criteria' section has a 'Forward In Time' toggle switch and a 'FROM EVENT NUMBER' field with a dropdown menu. Below these is a 'Network Filter' section. At the bottom of the dialog box are three buttons: 'Apply', 'Remove All Filters', and 'Close'. The event log table below the dialog box has columns for 'ID', 'Date/Time', 'IP Address', and 'Description'. It shows a list of events with status indicators (green checkmarks for 'reconnected' and red X's for 'disconnected').

ID	Date/Time	IP Address	Description
250185	Sep 25, 2018 2:43:54 PM	10.132.56.130	Device 10.132.56.130 reconnected
250184	Sep 25, 2018 2:43:31 PM	10.132.56.130	Device 10.132.56.130 disconnected
249681	Sep 25, 2018 10:09:08 AM	10.132.56.130	Device 10.132.56.130 reconnected
247434	Sep 24, 2018 3:30:30 PM	10.132.59.165	Device 10.132.59.165 reconnected
247246	Sep 24, 2018 1:57:54 PM	10.132.59.165	Device 10.132.59.165 disconnected
247245	Sep 24, 2018 1:57:12 PM	10.132.59.165	Device 10.132.59.165 reconnected
247180	Sep 24, 2018 1:24:42 PM	192.168.1.20	Device 192.168.1.20 reconnected
247179	Sep 24, 2018 1:24:17 PM	10.132.58.111	Device 10.132.58.111 reconnected
247178	Sep 24, 2018 1:24:17 PM	10.132.58.111	Device 10.132.58.111 reconnected
247177	Sep 24, 2018 1:24:17 PM	10.132.58.111	Device 10.132.58.111 reconnected
247170	Sep 24, 2018 1:23:03 PM	10.132.58.111	Device 10.132.58.111 disconnected
247169	Sep 24, 2018 1:23:03 PM	10.132.58.111	Device 10.132.58.111 disconnected
247168	Sep 24, 2018 1:23:03 PM	10.132.58.111	Device 10.132.58.111 disconnected
247161	Sep 24, 2018 1:20:10 PM	10.132.58.111	Device 10.132.58.111 reconnected
247160	Sep 24, 2018 1:20:10 PM	192.168.1.20	Device 192.168.1.20 disconnected
247159	Sep 24, 2018 1:20:10 PM	10.132.58.111	Device 10.132.58.111 reconnected

2. The filter option will glow, indicating the filter was applied, and all applicable events will be affected.
3. Close filter.

## Selection Criteria and Network Filter

Select the Filter option and scroll to find Selection Criteria and Network Filter. With this option, you can easily sort through your data.

1. Scroll down to find Selection Criteria and enter the appropriate **Event ID**.
2. Enter **From Date** information.

The screenshot shows the IntraVUE Event Log interface. The main table lists events with columns for ID, Date/Time, IP Address, and Description. The IP Address column contains links to device details. A sidebar on the right contains filter options. Two red arrows point from the table to the sidebar: one to the 'Type to filter events...' search bar and another to the 'Network Filter' section.

ID	Date/Time	IP Address	Description
✓ 250185	Sep 25, 2018 2:43:54 PM	<a href="#">10.132.56.130</a>	Device 10.132.56.130 reconnected
✗ 250184	Sep 25, 2018 2:43:31 PM	<a href="#">10.132.56.130</a>	Device 10.132.56.130 disconnected
✓ 249681	Sep 25, 2018 10:09:08 AM	<a href="#">10.132.56.130</a>	Device 10.132.56.130 reconnected
✓ 247434	Sep 24, 2018 3:30:30 PM	<a href="#">10.132.59.165</a>	Device 10.132.59.165 reconnected
✗ 247246	Sep 24, 2018 1:57:54 PM	<a href="#">10.132.59.165</a>	Device 10.132.59.165 disconnected
✓ 247245	Sep 24, 2018 1:57:12 PM	<a href="#">10.132.59.165</a>	Device 10.132.59.165 reconnected
✓ 247180	Sep 24, 2018 1:24:42 PM	<a href="#">192.168.1.20</a>	Device 192.168.1.20 reconnected
✓ 247179	Sep 24, 2018 1:24:17 PM	<a href="#">10.132.58.111</a>	Device 10.132.58.111 reconnected
✓ 247178	Sep 24, 2018 1:24:17 PM	<a href="#">10.132.58.111</a>	Device 10.132.58.111 reconnected
✓ 247177	Sep 24, 2018 1:24:17 PM	<a href="#">10.132.58.111</a>	Device 10.132.58.111 reconnected
✗ 247170	Sep 24, 2018 1:23:03 PM	<a href="#">10.132.58.111</a>	Device 10.132.58.111 disconnected
✗ 247169	Sep 24, 2018 1:23:03 PM	<a href="#">10.132.58.111</a>	Device 10.132.58.111 disconnected

**Selection Criteria**

- ☐ Forward In Time
- FROM EVENT NUMBER: Event ID
- FROM DATE: [Dropdown]

**Network Filter**

Type to filter data... [Select All] [Unselect All]

- ☐ 56
- ☐ 192
- ☐ 57
- ☐ 58
- ☐ 59

[Apply] [Remove All Filters] [Close]

- Under Network Filter, type the appropriate filter data.
- Select the desired network.
- Click **Apply** and **Close** when complete.

## Device Filter

Select the Filter option and scroll down to find **Device Filter**. With this option, you can sort data depending on the IP address or device name.

- Scroll down to find **Device Filter** and enter what data should be filtered.
- Under the SORTED BY section, decide whether to sort data through IP address or device name. Mark which option you choose.

The screenshot shows the IntraVUE software interface. The top navigation bar includes 'IntraVUE', 'Configure', 'View', 'Analyze', and 'Help'. Below this, a secondary bar contains 'Topology', 'Plant Layout', 'Device List', 'Filters', 'Event Log' (which is selected), and 'Diagnostics'. The main area displays an event log table with columns: ID, Date/Time, IP Address, and Description. A single event is listed with ID 81589, dated May 13, 2018 5:55:24 AM, IP Address 10.132.37.5, and Description 'Device 10.132.37.5 disconnected'. A 'Device Filter' dialog box is open on the right, featuring a search bar, 'Select All' and 'Unselect All' buttons, a 'SORTED BY' dropdown set to 'IP Address', and a list of devices with toggle switches. The device '10.132.37.5 - PLN-3560G-02.panduitlabs.com' is selected. At the bottom of the dialog are 'Apply', 'Remove All Filters', and 'Close' buttons.

ID	Date/Time	IP Address	Description
81589	May 13, 2018 5:55:24 AM	10.132.37.5	Device 10.132.37.5 disconnected

**Device Filter**

Type to filter data... [Select All] [Unselect All]

SORTED BY  
IP Address Device Name

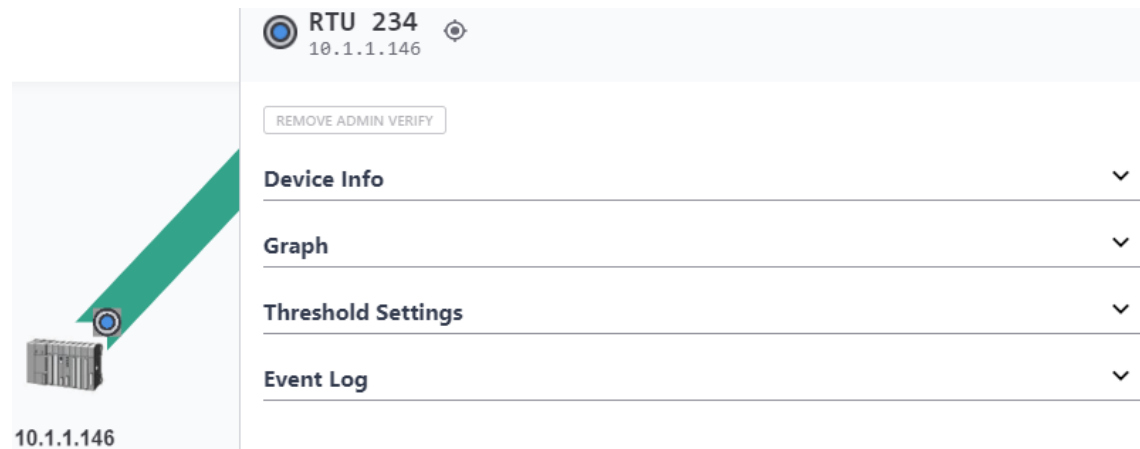
- ☐ 10.132.37.1 - PLN-IA-4507-1W-A.panduitlabs.com
- ☐ 10.132.37.3 - PLN-3560G-01.panduitlabs.com
- ☒ 10.132.37.5 - PLN-3560G-02.panduitlabs.com
- ☐ 10.132.37.79 - HMI1
- ☐ 10.132.37.80 - pln-ia-gen5PDU
- ☐ 10.132.37.81 - no name
- ☐ 10.132.37.92 - no name

[Apply] [Remove All Filters] [Close]

3. Click **Apply** and **Close** when complete.

## Device Side View

When you single click a device the right-side view will automatically slide on the right side of the screen which will show device information on the different four sections. To make it to relate IntraVUE™ information for that device to what you know for that device, the device name and IP address are frozen on the top even when you scroll up and down.



Four functions will always be present without logging in:

**Device Info:** The Properties for this device. This section displays some fixed information about the selected device obtained from devices through SNMP, and some extra SNMP data that may have been configured for this device by the administrator. See - [Side View in Edit Mode](#)

**Graph:** Threshold Graphs showing Ping and Bandwidth threshold for this device. See [Threshold Graphs](#)

**Threshold Settings:** Ping and Bandwidth set values. See [Configure Menu - Scanner Tab](#) to customize these values as necessary.

**Event Log:** The Event Log showing events for this device only and it follows the same color-coded format on the rest of the System Menu views. See [IntraVUE Legend](#)

The "Edit" button of the Side View will be disabled until you log in into IntraVUE™. See



## Connection Side View

PLN-SSRG-4510-1X-A.p...  
10.132.57.1 : 153  
GigabitEthernet2/25

→ PLN-SSRG-PVIQ-1X-1A-...  
10.132.57.201

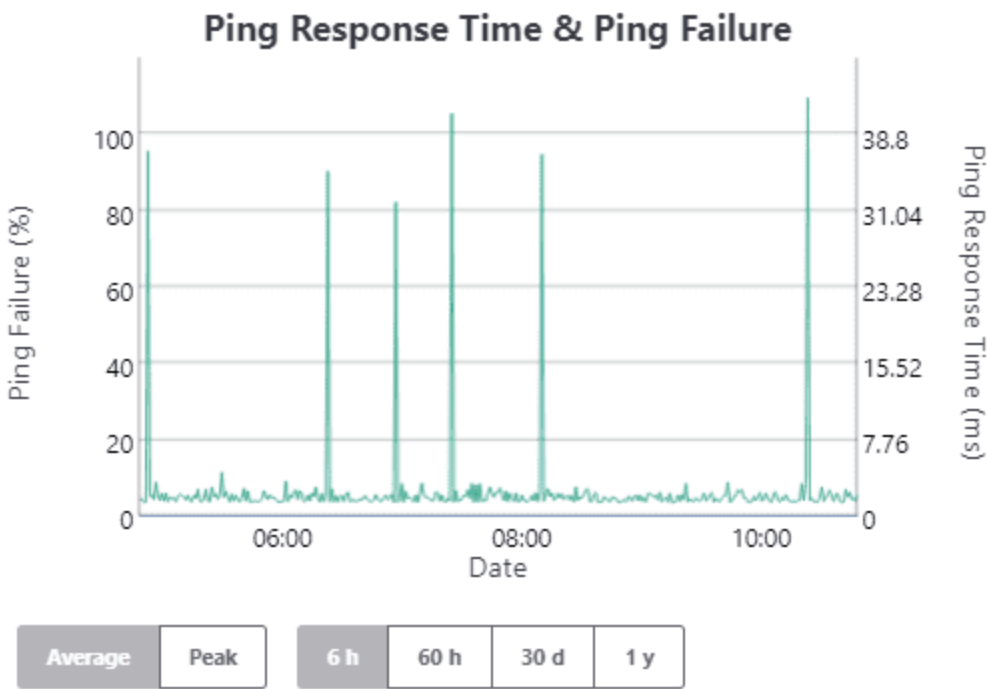
EDIT

— Connected

SNMP Status : Responding  
Link Speed : 100 Mbps

Ping Response/Failure Graph

^



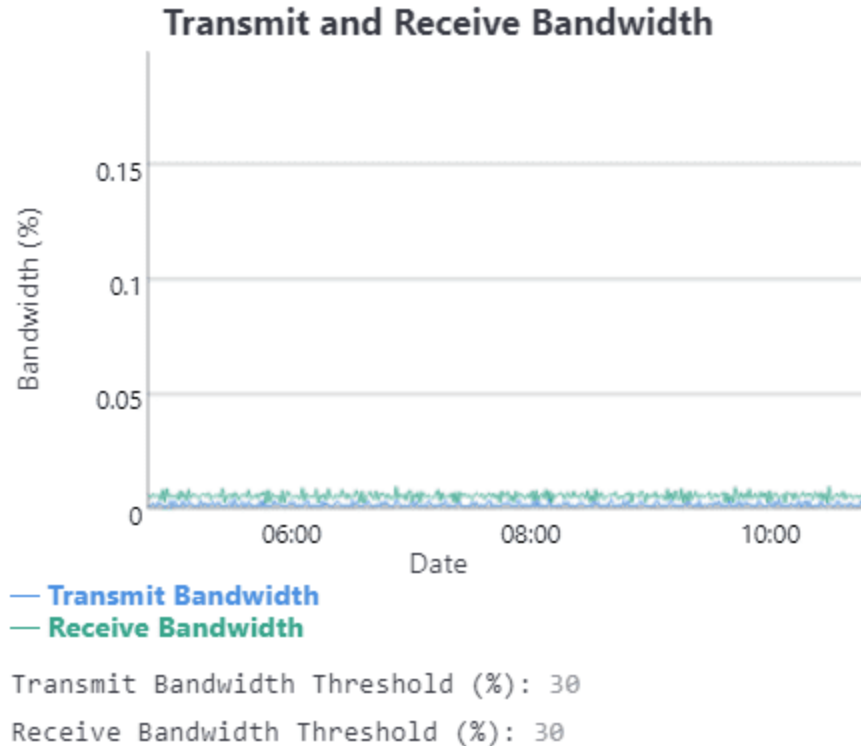
— Ping Failure  
— Ping Response Time

Ping Response Time Threshold (msec): 30  
Ping Failure Threshold (%): 20

---

**Transmit/Receive Bandwidth Graph**

---

**SNMP Status**

SNMP status for this device on the attached port. If the SNMP status is "Not Open" it may be due to SNMP being lost, blocked, or the device is not connected to a managed switch. See also

[IntraVUE Legend](#) , [Verifying SNMP on Fully Managed Switches](#)

**Link speed Info**

The current link speed for the device is shown at the very top, along with which end of the connection is the data source for the graph. Changes in link speed are recorded in the event log. Only devices having SNMP will have link speed data.

**Ping Failure & Ping Failure Threshold**

See [FAQs](#) , [IntraVUE Analytics](#) , [Threshold Graphs](#) , and [Configure Menu - Advanced Tab](#)

**Ping Response Time & Ping Response Time Threshold**

---

See [IntraVUE Diagnostics](#), [FAQs](#) , [IntraVUE Analytics](#), [Threshold Graphs](#), and [Configure Menu - Advanced Tab](#)

#### **Transmit Bandwidth & Transmit Bandwidth Threshold**

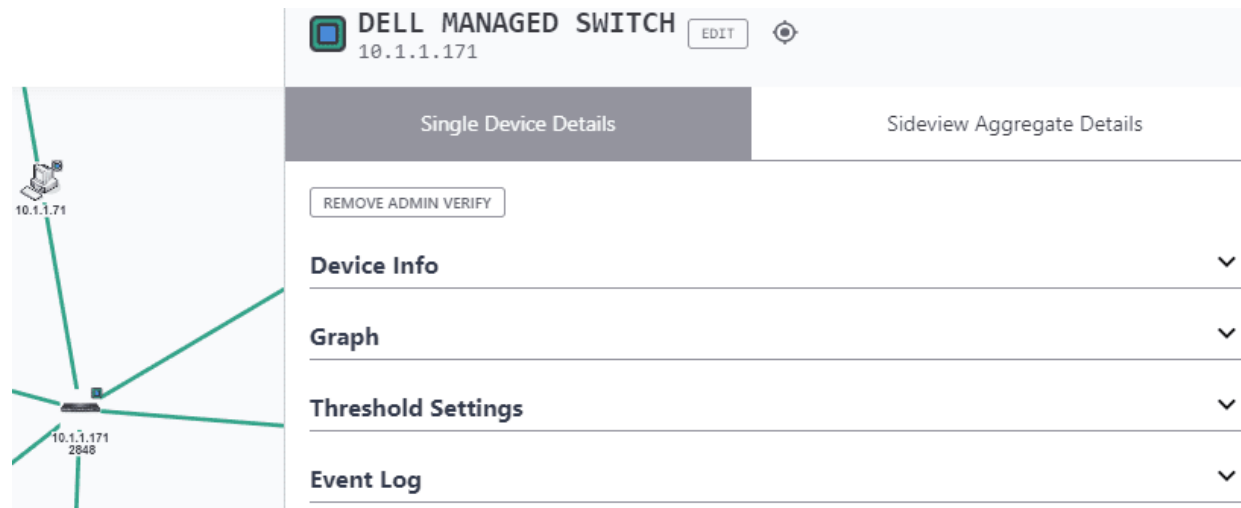
See [IntraVUE Diagnostics](#), [FAQs](#) , [IntraVUE Analytics](#), [Threshold Graphs](#), and [Configure Menu - Advanced Tab](#)

#### **Received Bandwidth & Received Bandwidth Threshold**

See [IntraVUE Diagnostics](#), [FAQs](#) , [IntraVUE Analytics](#), [Threshold Graphs](#), and [Configure Menu - Advanced Tab](#)

## Switch Side View

This view shows device information as well as ping and bandwidth information. This view is not restricted to switches but devices that have child nodes (e.g. hubs, hypervisors, APs, PLCs).



There is a side view dedicated for switches broken into two parts.

### Single Device Details

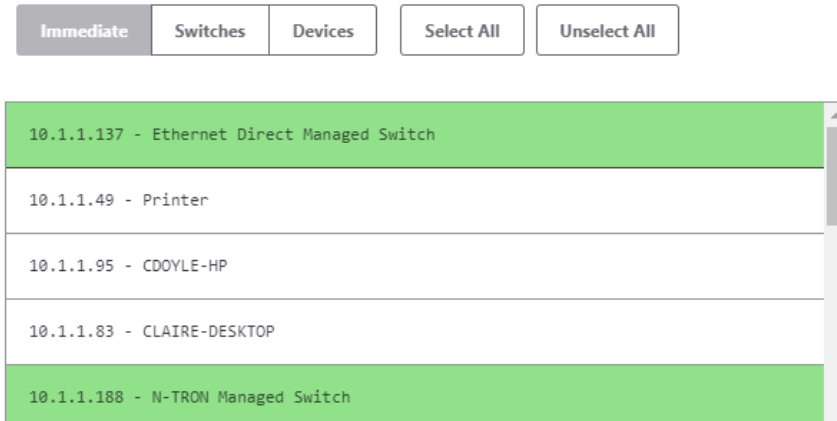
Contains to standard device properties. See [Device Side View](#)

### Sideview Aggregate Details

Contains ping and bandwidth data (commulative) for all devices connected to this device including:

It also has a muti-device threshold graph where you can analyze how the ping and bandwidth data behavior for child nodes. See [Threshold Graphs](#) to learn more about these graphs.

At the bottom of the side view there is a device selector containing one entry for each of the connected children showing its IP address and Device Name.



To alter the behavior of the multi-device graph select one of the following button combinations:

Pick a Type:

**Intermediate:** The Multi-Device Graph calculates and shows history for both switches and devices

**Switches:** The Multi-Device Graph calculates and shows history for switches only

**Devices:** The Multi-Device Graph calculates and shows history for devices only

Pick a Range:

**Select All:** Selects all devices for the type above

**Unselect All:** Unselects all devices for the type above



You can also manually select individual nodes by first clicking "Unselect All" then manually selecting just the devices you want in the Muti-Device Graph

## Selection

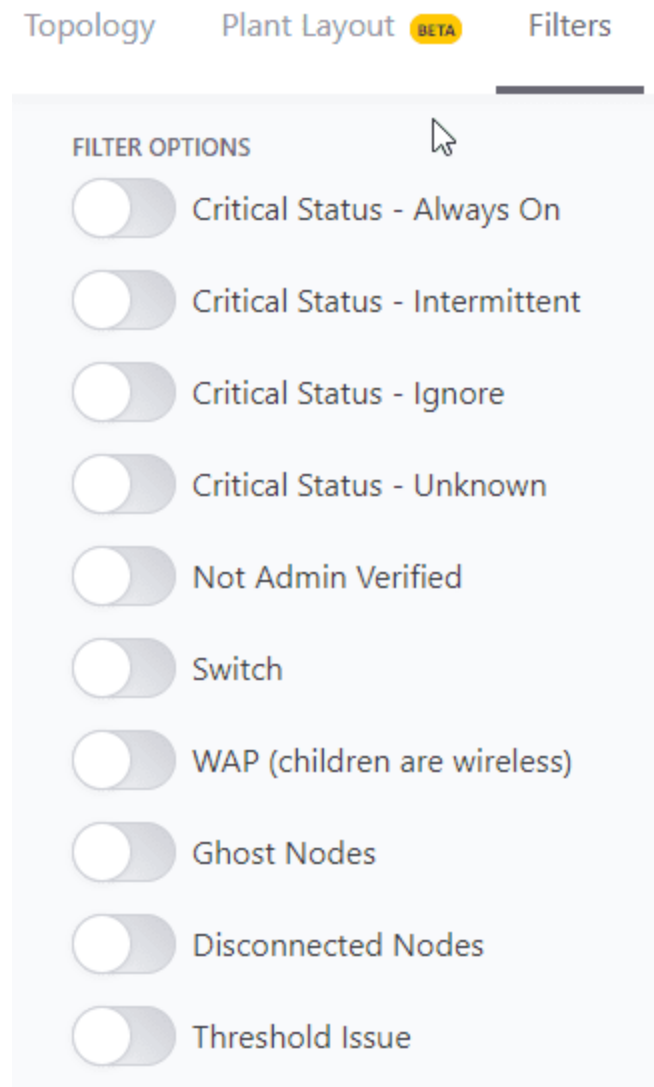
The main method of selection is clicking on a device showing child nodes. In this case all the devices connected to and below this device relative to the IntraVUE™ host computer are displayed together.

- » If you click on the IntraVUE™ host you will get all devices for a single network.
- » If you click on a top parent, you will get just the devices for that IntraVUE™ network.
- » If you click on a switch, you will get just that switch and the devices below that switch.

An alternate method of selection is to select several devices and this will allow you to view just the selected devices in the Multiple Device Side View.

## View Filters

IntraVUE™ provides a granular filters to make it easier for users to identify automation devices.



Some filters may require devices to be previously configured for the specific filter to work. See additional details.

- **Critical Status** (device must already be configured with this setting). See [Device Configure - General](#)

- **Non-Admin Verified**. See [Admin Verification in IntraVUE 3](#)

-**Switches** - these would be fully managed switches. See [Verifying SNMP on Fully Managed Switches](#)

-**Wireless Access Point (WAP)**. See [Device Configuration - Advanced Tab](#)

-**Ghost Nodes**. See [Admin Verification in IntraVUE 3](#)

-**Disconnected Nodes** - See [IntraVUE Legend](#)

-**Threshold Issue**. Bandwidth / Ping issue . See [Threshold Graphs](#)

### Device Filters

These filters are designed to provide a direct eye-bird view to applicable devices of the selected filter. You can pick more than 2 filters at a time. The view filters apply to the Topology, Plant Layout, and List views.

Enable Device Filters :

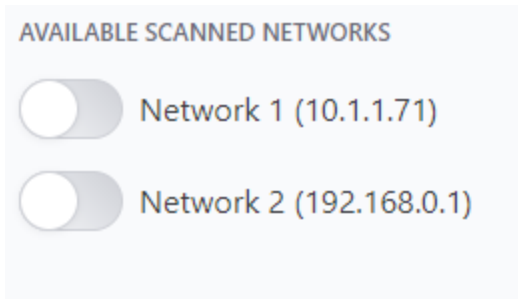
1. Apply one of the these view filters
2. Return to either the Topology, Plant Layout, or List View and notice the nodes "highlighted" while the rest of the nodes are grayed out. You will see a blue navigation bar with message "You are currently viewing a filtered view of devices".

Remove Device Filters:

1. Click on any of the two buttons "Change Filters" or "Remove Device Filters" on the blue navigation bar, or return to the Filters tab and un-check the previously selected device filters to reset the views.

### Available Scanned Networks Filters

IntraVUE™ can allow you to isolate the view by filtering by enabling only one or multiple specific networks from the "Available Scanned Networks" section in Filters.



You can combine both filter options and available scanned networks filters to make it easy to diagnose, document, or analyze your network.

Enable Available Scanned Network Filters:

1. Apply one of the these filters
2. Return to either the Topology, Plant Layout, Event Log, or Diagnostics View and notice that the selected IntraVUE™ network or networks are mapped out. You will see a blue navigation bar with message "You are currently viewing a subset of scanned networks".

Remove Available Scanned Network Filters:

1. Click on any of the two buttons "Change Filters" or "Remove Device Filters" on the blue navigation bar on top, or return to the Filters section and un-check the previously selected device filters to reset the views.



# Diagnostics View

In this view IntraVUE™ allows you to see **CRC**<sup>1</sup> errors from devices including their IP address, Network Name, Device Name, Physical port name description, and type of diagnostics error, value, error time, and error time since now.

The type of errors that IntraVUE™ can detect for a port can be either **CRC**<sup>2</sup>, or IfInErrors are shown for devices supporting the standard MIB.

The Show Server Time check box is available.

Port Descriptions (e.g. FastEthernet0/2) are displayed for connection lines.

---

<sup>1</sup>he cyclic redundancy check (CRC) is a technique used to detect errors in digital data. CRC is a hash function that detects accidental changes to raw computer data commonly used in digital telecommunications networks and storage devices such as hard disk drives. This technique was invented by W. Wesley Peterson in 1961 and further developed by the CCITT (Comité Consultatif International Telegraphique et Telephonique). Cyclic redundancy checks are quite simple to implement in hardware and can be easily analyzed mathematically. It is one of the better techniques in detecting common transmission errors. It is based on binary division and is also called polynomial code checksum.

<sup>2</sup>he cyclic redundancy check (CRC) is a technique used to detect errors in digital data. CRC is a hash function that detects accidental changes to raw computer data commonly used in digital telecommunications networks and storage devices such as hard disk drives. This technique was invented by W. Wesley Peterson in 1961 and further developed by the CCITT (Comité Consultatif International Telegraphique et Telephonique). Cyclic redundancy checks are quite simple to implement in hardware and can be easily analyzed mathematically. It is one of the better techniques in detecting common transmission errors. It is based on binary division and is also called polynomial code checksum.

Warning - data is not current. Scanner is in OFFLINE mode. Demonstration Version - Not for Commercial Use.									
IntraVUE Configure View Analyze Help									
Topology Plant Layout <b>1816</b> Device List Filters Event Log Diagnostics									
Type to filter data...									
IP Address	Device Name	Port Description	Port Number	Network Name	In Errors	In Errors Time	In Errors Last Changed	CRC Align Errors	CRC Align Errors Time
<a href="#">192.168.58.153</a>	DEMO-LAB-Switch-03	<a href="#">FastEthernet1/19</a>	<a href="#">19</a>	Network-58	1	Sep 17, 2018 8:03:41 AM	8 days ago	--	--
<a href="#">192.168.58.151</a>	DEMO-LAB-Switch-01	<a href="#">FastEthernet1/4</a>	<a href="#">6</a>	Network-58	2	Sep 17, 2018 1:19:45 PM	8 days ago	--	--
<a href="#">192.168.58.151</a>	DEMO-LAB-Switch-01	<a href="#">GigabitEthernet1/2</a>	<a href="#">2</a>	Network-58	1	Aug 31, 2018 11:47:05 AM	25 days ago	--	--
<a href="#">192.168.58.152</a>	DEMO-LAB-Switch-02	<a href="#">FastEthernet1/5</a>	<a href="#">7</a>	Network-58	5	Sep 17, 2018 1:25:45 PM	8 days ago	--	--
<a href="#">192.168.58.152</a>	DEMO-LAB-Switch-02	FastEthernet1/8	10	Network-58	3	Sep 17, 2018 1:25:45 PM	8 days ago	--	--
<a href="#">192.168.57.14</a>	DEMO-LAB-5700-2.panduitlabs.com	<a href="#">FastEthernet1/19</a>	<a href="#">19</a>	Network-57	1	Sep 17, 2018 3:07:46 PM	8 days ago	--	--
<a href="#">192.168.57.15</a>	DEMO-LAB-hirsch-A	<a href="#">Module 1 Port 3 - 10/100 Mbit TX</a>	<a href="#">3</a>	Network-57	17	Sep 18, 2018 3:07:47 PM	7 days ago	1	Sep 17, 2018 10:55:46
<a href="#">192.168.57.10</a>	DEMO-LAB-8300.panduitlabs.com	GigabitEthernet1/1	1	Network-57	1	Sep 17, 2018 3:07:46 PM	8 days ago	--	--
<a href="#">192.168.57.16</a>	DEMO-LAB-hirsch-B	<a href="#">Module 1 Port 1 - 10/100 Mbit TX</a>	<a href="#">1</a>	Network-57	152	Sep 18, 2018 4:01:47 PM	7 days ago	39	Sep 18, 2018 3:07:47 P
<a href="#">192.168.57.17</a>	DEMO-LAB-hirsch-C	<a href="#">Module 1 Port 3 - 10/100 Mbit TX</a>	<a href="#">3</a>	Network-57	17	Sep 18, 2018 1:13:48 PM	7 days ago	4	Sep 18, 2018 12:13:47
<a href="#">192.168.1.200</a>	GS108T-2		<a href="#">3</a>	Network-192	1	Sep 18, 2018 1:01:47 PM	7 days ago	0	Jul 11, 2018 1:47:16 PM
<a href="#">192.168.1.193</a>	065-7861POE	<a href="#">Port 19</a>	<a href="#">19</a>	Network-192	836	Sep 18, 2018 4:01:47 PM	7 days ago	--	--

- » By default, IntraVUE only retrieves CRC and IfnErrors from switches. CRC and IfnErrors data are not retrieved from devices by default. You may enable retrieval of CRC and IfnErrors from the devices by setting the `crc.getFromAllDevices=1` in the `ivserver.properties`.
- » When a IfnError or CRC Error occurs, the line will turn yellow and will remain yellow for the number of hours, by default one hour, before creating next event. This default can be changed in the `ivserver.properties` by setting the `CrcEventDelay` property for CRC events and `InputErrorsEventDelay` property for IfnError.



Selecting the IP address of a device will center that device in the Topology View.

In general CRC and IfnErrors show when frames are corrupted at the OSI Layer 2 and indicate problems such as:

- » Corruption or loss of data
- » Duplex mismatch
- » Faulty cabling
- » Broken hardware
- » End stations freezing

- » Equipment power resetting
- » Interface noise on network cabling segments (UTP, Copper, Fiber)
- » Errors at the transmitting or receiving end

However, some level of CRC errors should be expected and it's acceptable according to the CRC standard, and a very low rate is still acceptable (i.e. not greater than 1 percent of the total network traffic).

When a CRC Error occurs, the line will turn yellow and will remain yellow for the number of hours, then default one hour before creating next event.

## Roaming Devices

Devices can be configured by the Administrator to move from location to location without sending out an alarm when they become disconnected. These devices will be logged as to the changes and moves.

The Device will first appear to be disconnected and then, when it establishes communications at the new point, the old connection will be erased.

If the device is Admin Verified, the red filled box will not be created when the device is discovered at a new location, instead the blue filled box will just move to the new location.

Wireless devices will typically have this feature enabled to allow them to freely move within a facility without alarms.

To enable this feature check the Auto Connect checkbox in the Device Configuration dialog. See [Admin Verification in IntraVUE 3](#)

## Admin Functions

## Side View in Edit Mode

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click on any device. A slider bar will pop up on the right on the screen. This is your device properties panel.



If you haven't Admin Verified such devices click "Admin Verify". See [Admin Verification in IntraVUE 3](#)

3. While logged in as admin click "Edit". The Device Configuration dialog has 6 sections that allow you to configure the unique properties of a device.

<b>General</b>	^
<b>Other Names</b>	^
<b>Image</b>	^
<b>Advanced</b>	^
<b>SNMP</b>	^
<b>Links</b>	^

4. In the General Tab > Set a defined device name and location.
5. In the Other Names tab > Set additional defined names (i.e. function, description, owner ).
6. In the Image tab > Assign an image from the drop down.
7. In the Links tab > Fill in any documentation link (e.g. Administration Web link, Floor Layout, Maintenance user manual, wiring diagram, location pictures, various devices properties) for each URL NAME box that wasn't auto-detected by IntraVUE.
8. Click " Apply and Close"



Remember to save your changes before clicking on a different device as your changes will not be saved automatically.

9. Continue doing this for all end devices, switches, and the top parents (i.e. router, IntraVUE™ agent, and the IntraVUE™ host).

Tab	Description
General	Contains Admin Verification, wireless, SNMP, email, and other settings. See <a href="#">Device Configure - General</a>
Other Names	Allows you to set other devices names in the devices properties. See <a href="#">Device Configure - Other Names</a>
Image	Allows you to assign an image to a device. See <a href="#">Device Configuration - Image</a>
Advanced	Allows you to change device type and behavior on the map view. See <a href="#">Device Configuration - Advanced Tab</a>
SNMP	Allows you to enable or disable SNMP requests to a device. See <a href="#">Device Configure - SNMP</a>
Links	Allows you to assign Web Links to a device. See <a href="#">Device Configuration - Links</a>

## Device Configure - General

While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to preserve changes.



**Admin Verification** When this is checked, the position of the device is frozen or locked to its current position. If the device is moved, the IntraVUE browser will show a red filled circle at the verified position and a tan circle at the current location of the device. See a complete description about [Admin Verification in IntraVUE 3](#) and its benefits.

ADMIN VERIFY

### Device Info

You can also remove "Admin Verified" when you click again on the same button "Remove Admin Verify".

REMOVE ADMIN VERIFY

### Device Info

Click 'Edit' to access this tab.



**General**

DEVICE NAME

LOCATION

CRITICAL STATUS



SEND ALARMS

ALARM EMAIL ADDRESS



SEND ALARMS TO DEFAULT USER

**General**

The IP address name is set when a device is initially discovered and it can not be changed, even the 'n/a' nodes. See [Vendor Name from OUI](#) and [Device Discovery & Management](#)

You can enter a device name is not already configured as well as a location name.

**Critical Status**

Device Critical Status is set to one of the 4 critical values

CRITICAL STATUS



Unknown

Ignore

Intermittent

Always On

See [IntraVUE Analytics](#) for help on setting critical status.

## Send Alarms

If checked, any email alarms created by this device will go to the email address in under the button "Send Alarms".

To enable a large number of devices you can use the Export/Import technique using a spreadsheet. See Email Alarms under [Event Logging](#) to learn with events can generate an email alarm.

## Send Alarms to Default User

This button activates the default email of the user that gets email for this particular device. The "Enable Email" checkbox must be enabled and email SMTP server gateway must be previously configured under Configure > Email for this to work.

### NOTE:

You can have **IGNORE SNMP DEVICE NAME** or **IGNORE SNMP DEVICE LOCATION** checked and the scanner will not use SNMP to get a device's Device name and/or Location field. SEE [Device Configure - SNMP](#)

This is important for some devices which respond to SNMP but do not have a name or location configured.

Enter the value you want to use instead of what the device reports from SNMP.

## Device Configure - Other Names

You can assign additional names or modify the values found by IntraVUE™. While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to preserve changes.

### Other Names

---

USER DEFINED 1

USER DEFINED 2

USER DEFINED 3

REVISION

ENETIP Rev 1.02

VENDOR

Rockwell/Allen-Bradley

MODEL

1769-L33ERM/A LOGIX5333ERM

The IP address name is set when a device is initially discovered and it can not be changed, even the 'n/a' nodes.

The "User Defined" fields can be use to show custom values to a device such as Function of the Device, Description, Owner , etc. You can change the titles of these custom labels (e.g. from "User Defined 1" to "Engineering Team#" ). See [Device Configure - General](#).

Revision, Vendor, and Model names are usually auto-detected by SNMP if the devices has these out of factory or configured by someone. IntraVUE™ will automatically populate these fields if that is the case. See [Device Discovery & Management](#) to learn more about device information discovery.

### NOTE

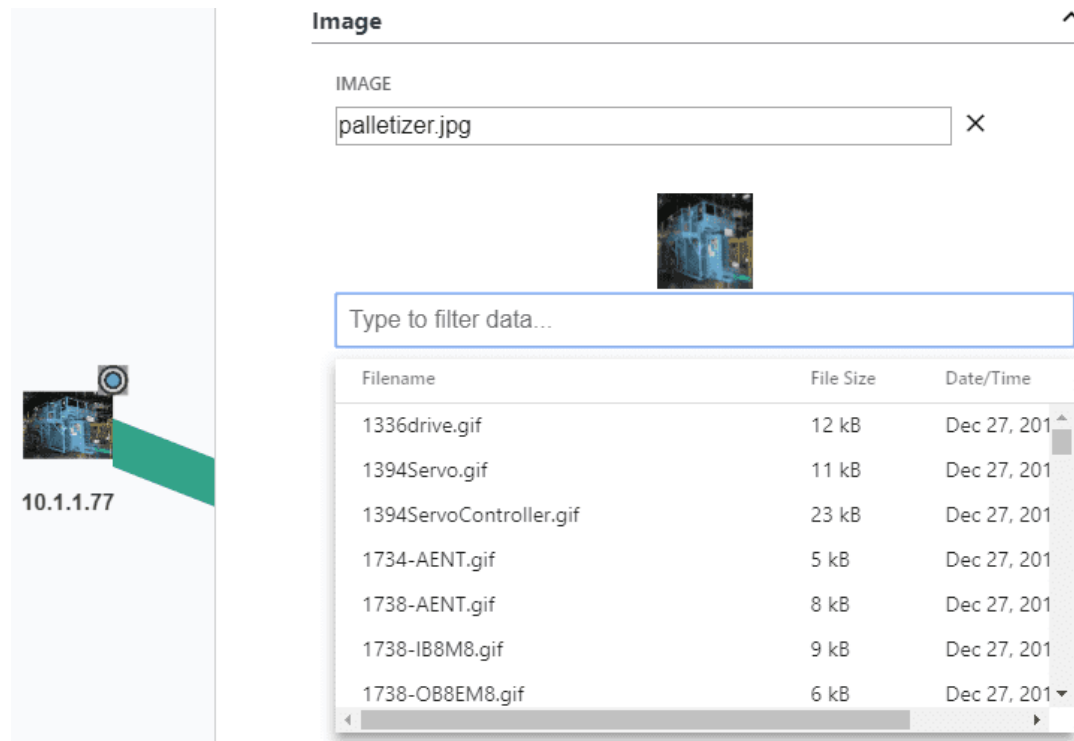
You can have **IGNORE SNMP BRIDGE MIB DATA** checked and the scanner will not attempt to use SNMP to get a device's Device Model, Vendor, and/or Revision field. See [Device Configure - SNMP](#)).

This is important for some devices which respond to SNMP but do not have a Device Model, Vendor, and/or Revision field configured.

Enter the value you want to use instead of what the device reports from SNMP.

## Device Configuration - Image

This tab allows you to assign an image of your choice from the available list of plant automation network devices included in the IntraVUE™ install. While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to pre-serve changes.



The image you assign will be permanent until you decide to replace this with another image, or remove the any image completely by clicking on the 'x' symbol.

You can also use the "Type to filter data" field to enter or paste text and navigate faster to a desired image name.



IntraVUE™ auto discovery does not add an image to a device automatically. This is a common misconception of the auto-discovery process for both SNMP-enabled devices and non-SNMP enabled devices.

To remove the assigned image from the device simply click on the 'x' and click "Save Changes" to apply the change.

The location of the images in the IntraVUE™ host is C:\intravue\autoip\tomcat8\webapps\ROOT\intravue\images. You can save images (i.e. jpg, png, and gif) directly to this folder. Simply exit and re-enter 'Edit' mode, then come back to the image section and you can now select the image from the list.

## Device Configuration - Advanced Tab

While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to preserve changes.

The screenshot displays the IntraVUE interface. On the left, a network diagram shows a connection between a green node labeled '1.49' and a yellow node labeled 'N/A\_397'. The interface includes a top bar with 'Filters' and 'Event Log' tabs. On the right, the configuration panel for 'SECCAM1' is open, featuring a 'CANCEL' button and a refresh icon. The panel is divided into sections: 'General', 'Other Names', 'Image', 'Advanced', 'SNMP', and 'Links'. The 'Advanced' section contains five toggle switches: 'AUTO CONNECT', 'AUTO IP', 'WAP (CHILDREN ARE WIRELESS)', 'VM, HUB, OR NON-SNMP SWITCH', and 'NAT'. Below these toggles are three buttons: 'Add Child Device', 'Delete this Device', and 'Move this Device'.

### Auto Connect

This feature works in conjunction with Admin Verification. Enabling this check box configures IntraVUE™ to treat this device as having permission to connect and disconnect from the different parts of the network without creating 'ghost nodes' (see Admin Verified below).

Examples of this are wireless devices that roam a plant or test devices that move from location to location. When a device with this feature enabled re-connects to the network it becomes active in its (perhaps new) location without admin action.

Laptop computers and other equipment that can be connected at a number of different locations should also have this feature enabled. The event log will still document all connections made and lost.

### **Auto IP**

Enabling this check box adds information about this device to a list of devices having IntraVUE™'s optional AutoIP BootP services. Note: if the device connects to a Cisco switch, you must edit the device configuration in AutoIP to a an @ with the VLAN number, like '@502' for VLAN 502.

AutoIP BootP server is a separate Software package that can be purchased to work with IntraVUE™. Please contact your local IntraVUE™ salesperson or go to the [IntraVUE Main page](#) for more information.

### **WAP (all children wireless)**

Enabling this check box causes any children of this device to have a dashed line using the color that is appropriate for its line condition. This is automatically checked if the device is discovered to be a Wireless Access Point.

### **VM, HUB, or NON-SNMP SWITCH**

The checkbox will cause all peer on the same port of the parent, managed switch, to become children of this device. It is provided as a convenience to using the MOVE function and works as new devices are discovered. Wireless APs should also have the WAP checkbox checked. A host computer with Virtual Machines can use this to make the VM sessions appear below the host PC.

### **NAT**

This setting suppresses the automatic merge that would normally happen if multiple devices appear to have the same MAC (as is common when operating through NAT devices).

### **Add Child Device**

To add a child to a parent node login as admin, click on a parent node, go to 'Edit', and under Advanced click "Add Child Device" manually to add a node. Wait for IntraVUE™ to add the child will cause a manually inserted node to be added to the selected device. Manually inserted nodes will



have "N/A" as the initial setting for all device views. These are capital letters to distinguish them from automatically inserted nodes which are in lower case letters, "n/a". This is typically used for devices connected via linking devices. The properties of the new node can be changed to reflect a device which is in the network but not visible to the scan engine. Typically, the other devices that are physically connected to the inserted node will be moved graphically to the new node using the MOVE function. An event log entry is generated for this operation. There will be a black connecting line to one of these nodes until a device which is responding to pings is moved under them. (You can not change the "N/A" in the IP View but you may change all the other device names).

### Delete this Device

To delete a device login as admin, click on the device, go to 'Edit', and under Advanced click "Delete this Device" manually delete this node. Click "Confirm Delete" to proceed with the deletion. Wait for IntraVUE™ to remove the device from the view will remove the device and delete it from the database. NOTE: if the device's IP address is in the scan range the device will be rediscovered as soon as it responds to a ping.



**Delete These Devices:** When logged in as an admin you can delete multiple devices with a single click. See [Multiple Device Side View](#)

### Move this Device

Move allows the user to change the parent of a device. To move a device login as admin and click on the device, go to 'Edit', and under Advanced click "Move this Device" to manually move this node. Click on the target switch and wait for "Move Device? Yes No" confirmation on the navigation bar. Click "Yes" to proceed with the move. Wait for IntraVUE™ to move the device from the old parent to the new parent node.

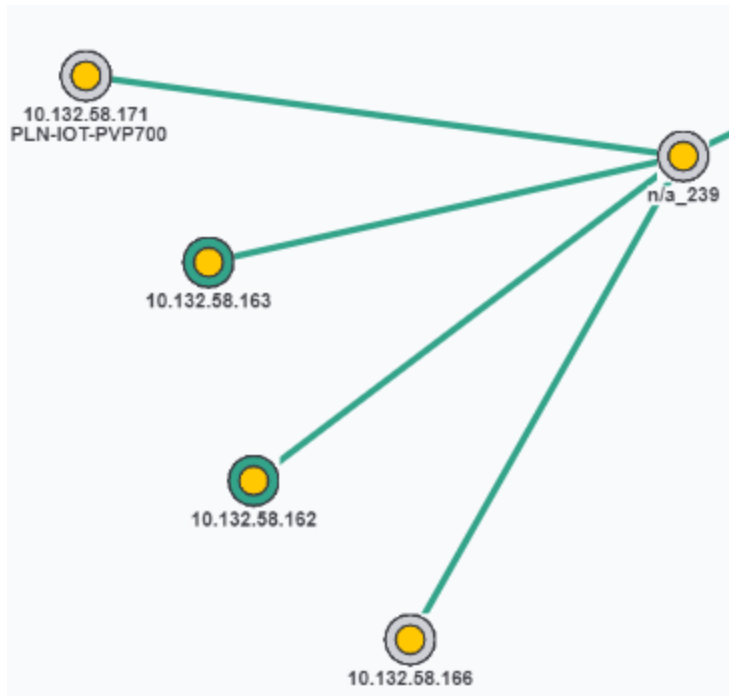
There are several occasions when you may want to manually change the relationship between the devices shown on the IntraVUE™ browser window.

- » You want to show non-IP address devices such as a copper to fiber media converter.
- » You want show non-Ethernet devices such as serial devices that are connected through an Ethernet-to-Serial converter.

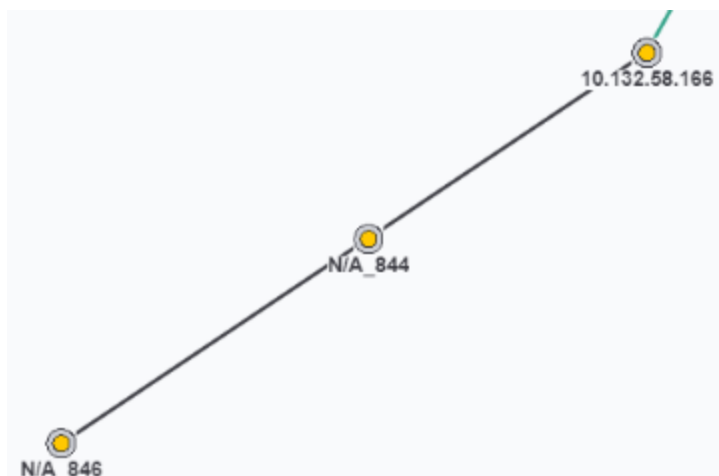
## Media Converters

Media Converters typically do not have IP addresses. They may take the copper CAT5 cable and convert it to fiber or even wireless. A second device typically converts the signal back to copper.

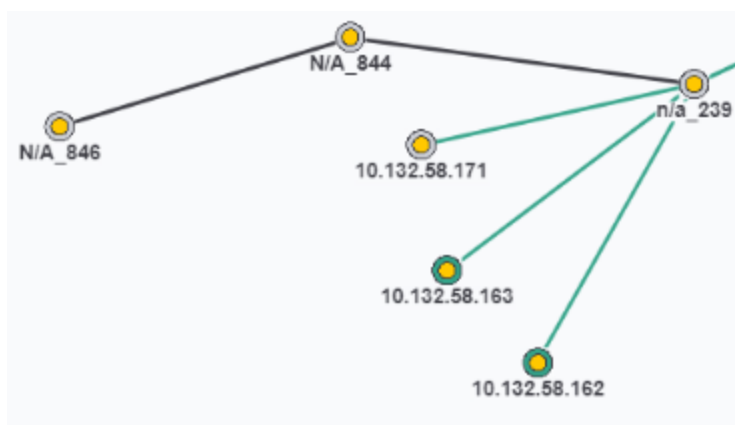
When doing this it is desirable to have the port of the managed switch be maintained. In the image below there is a port number for the line connecting the device.



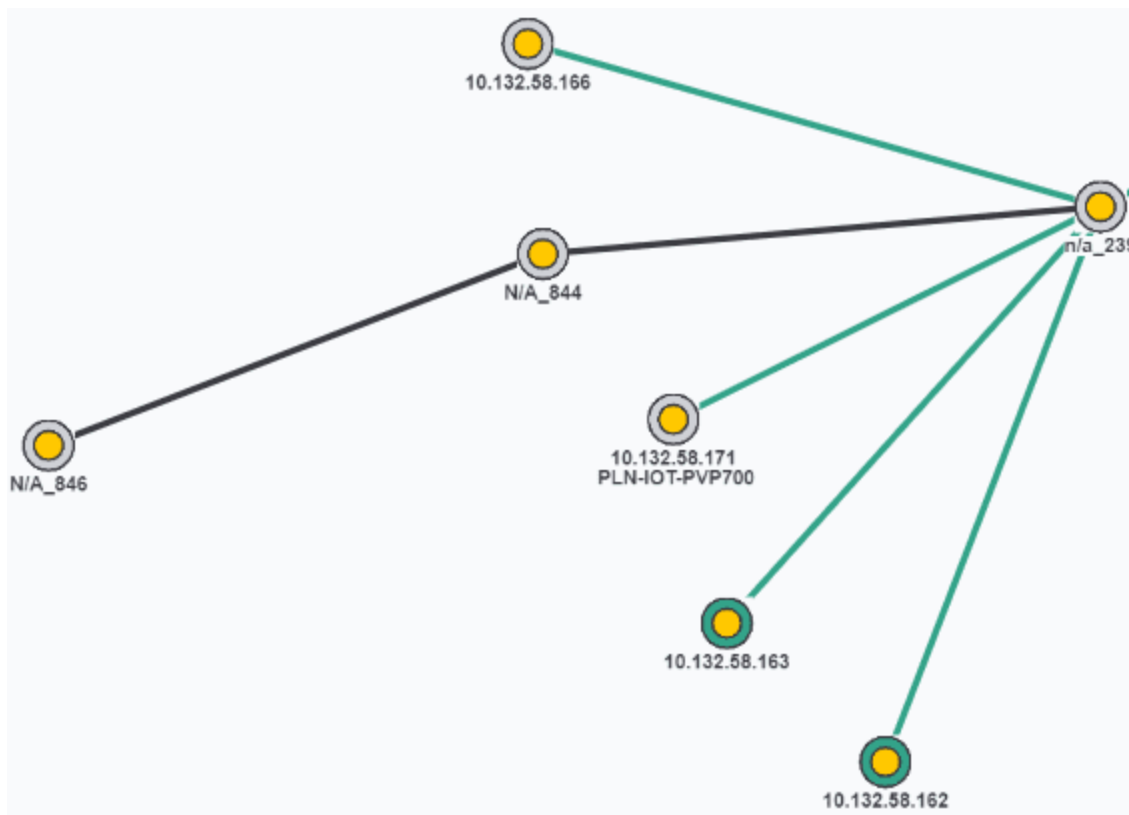
Use Add Child and add a child first to the device, and next to the just added child. You now have two unnamed child devices under the original device.



Now Delete the device with the IP address.



It will be rediscovered and become a child under a NEW auto-inserted node, at its original location. Next select the device (it gets a blue outline) and use Configure on the lowest child to MOVE the device below that node.



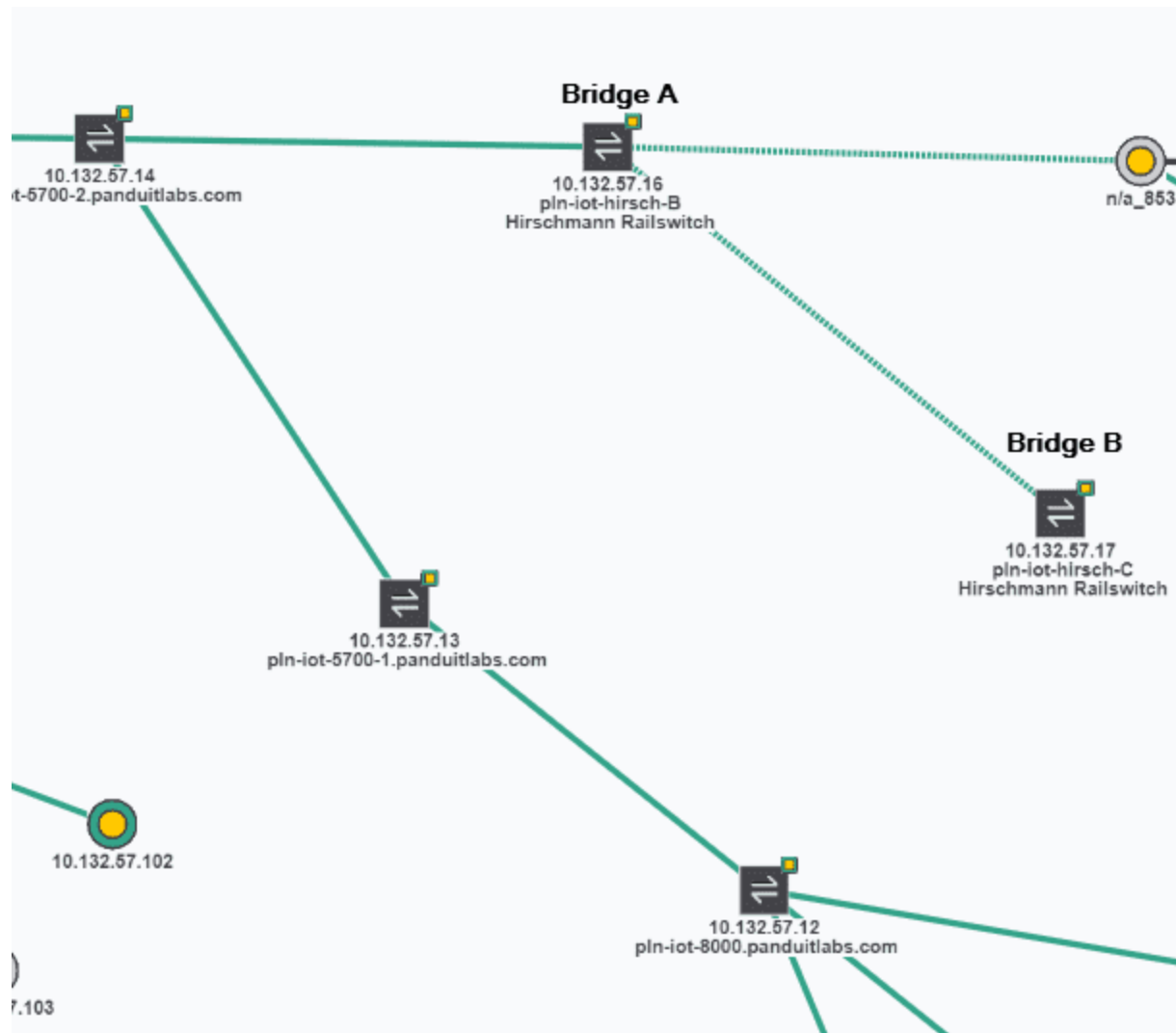
The auto-inserted node will go away, the connecting line to the first node will still have a port number, and the additional device nodes will help you understand your network when problems arise.



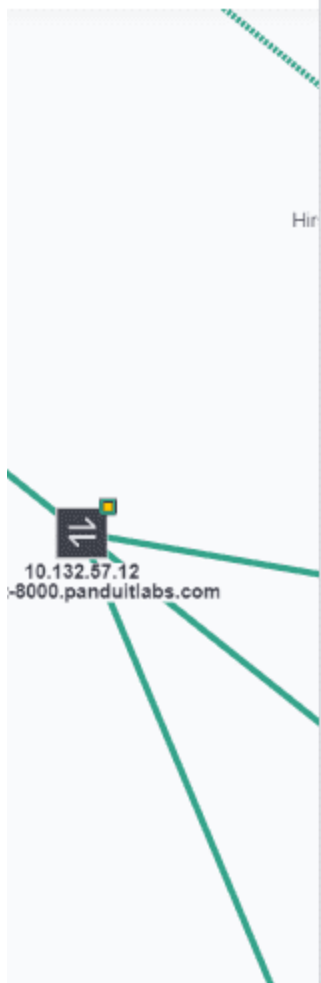
### Example of Configuring a Bridge

In the image below, the .16 and .17 devices have been discovered as wireless bridges. IntraVUE™ will not know which ip address is on the IntraVUE™ side of the network so you could find either one as the parent.

The devices on the other side of the bridge will appear under the top bridge, along with the other end of the bridge.




In this case, the .17 is on the IntraVUE™ side and we want the devices, starting with the .12, to appear under Bridge B, the .17, needs to get the devices so we use the Move instructions above. Select the .12 then move to, the .17.



The network diagram on the left shows a central bridge icon with a double-headed arrow. It is connected to several other devices represented by small squares. One device is labeled with the IP address 10.132.57.12 and the domain -8000.panduitlabs.com. The bridge is also connected to a device labeled 'Hir'.

**PLN-IOT-8000.PANDUITLABS.COM**  
10.132.57.12



☐ SEND ALARMS TO DEFAULT USER

**Other Names**

**Image**

**Advanced**

☐ AUTO CONNECT

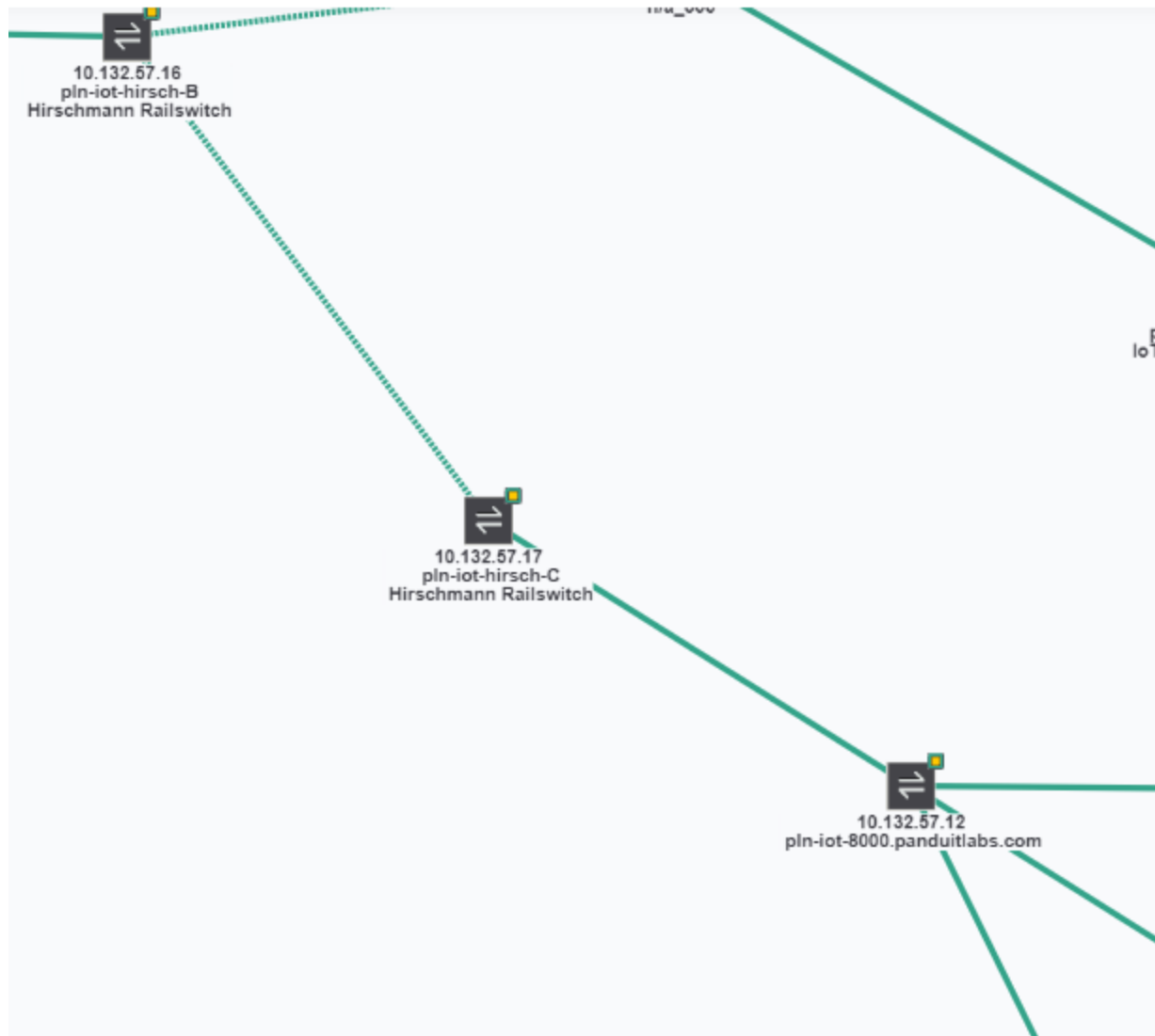
☐ AUTO IP

☐ WAP (CHILDREN ARE WIRELESS)

☐ VM, HUB, OR NON-SNMP SWITCH

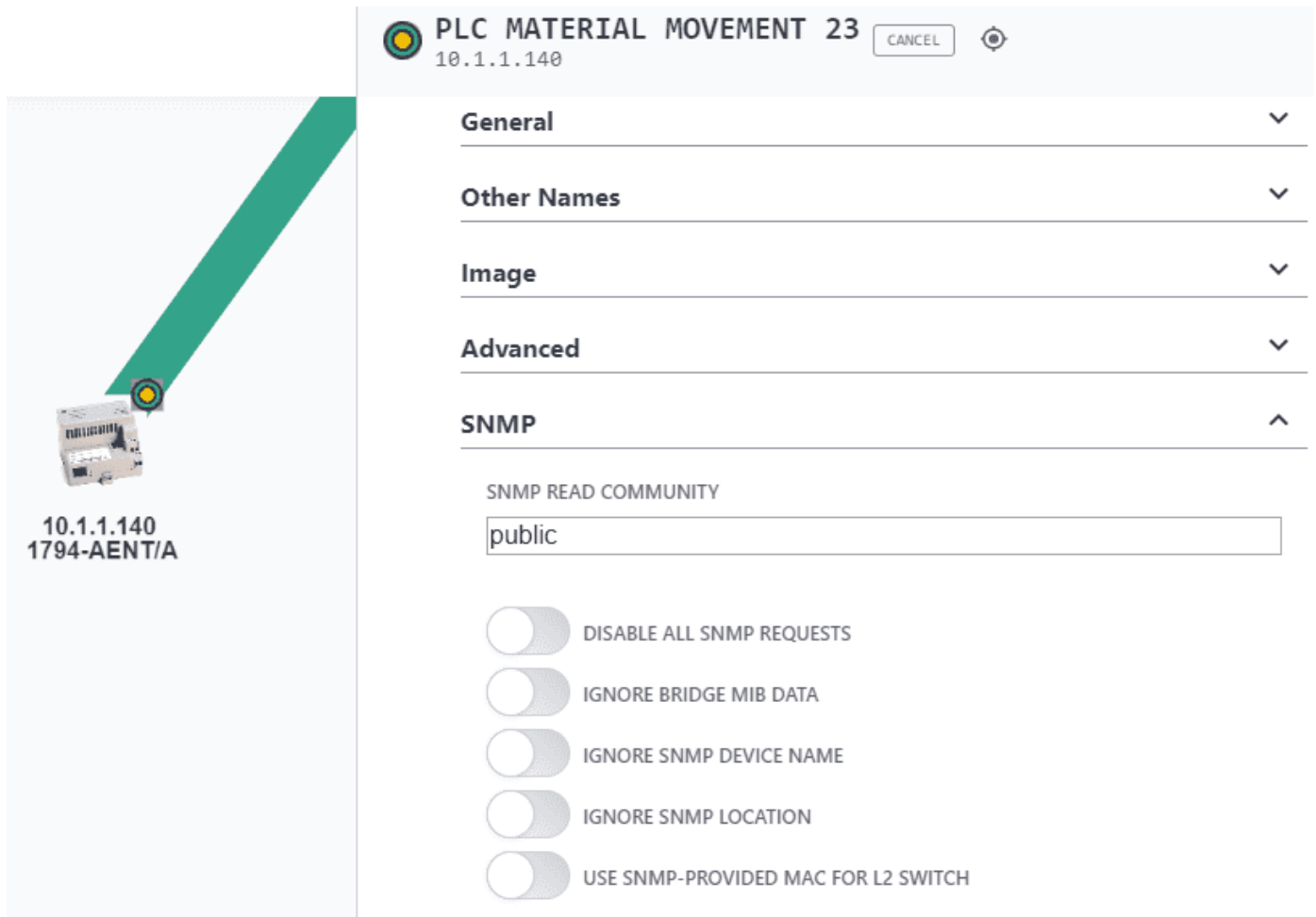
☐ NAT

The devices on the other side of the bridge will now be under the .17.



## Device Configure - SNMP

While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to preserve changes.



**PLC MATERIAL MOVEMENT 23** 10.1.1.140 CANCEL

**General** ▼

**Other Names** ▼

**Image** ▼

**Advanced** ▼

**SNMP** ▲

SNMP READ COMMUNITY

☐ DISABLE ALL SNMP REQUESTS

☐ IGNORE BRIDGE MIB DATA

☐ IGNORE SNMP DEVICE NAME

☐ IGNORE SNMP LOCATION

☐ USE SNMP-PROVIDED MAC FOR L2 SWITCH

### SNMP Read Community

This is the SNMP community to use in communicating with this device. It **MUST** be correct for any managed switches in order for the topology to be discovered. If it is not set for a switch, the switch and the devices connected to the switch will appear together under an auto-inserted node (n/a node).

This value will only be automatically set upon successful SNMP communication based on the value in the System Config Scanner dialog. If you have many devices with non-default SNMP communities, you will be able to change the default in the Scanner dialog for a short period and let



devices with that community get discovered and configured. Then you can change the community in the Scanner dialog back to the default.

### **Disable All SNMP Requests**

This is used to stop poorly performing SNMP devices from filling the event log file with SNMP lost and gained messages or to prevent SNMP to devices that would otherwise cause authentication traps to be issued when the IntraVUE admin does not have access to its read only community.

### **Ignore SNMP Bridge Mib data**

This is used for managed switches with poor snmp implementation. It is typically used in conjunction with the 'Unmanaged Switch or Wireless AP' checkbox.

### **Ignore SNMP Device Name**

Using this setting prevents the scanner from getting the SNMP Device Name from the device

### **Ignore SNMP Location**

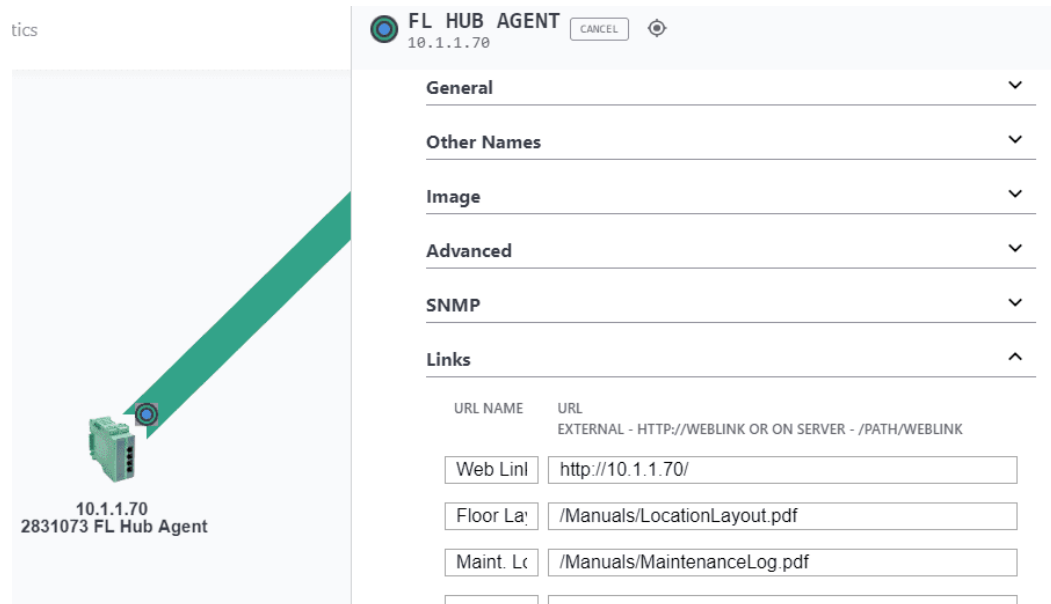
Using this setting prevents the scanner from getting the SNMP Location from the device

### **Use SNMP provided MAC for L2 Switch**

This checkbox allows a the IntraVUE scanner to get the MAC Address of a switch in a different subnet without having SNMP access to the router of that subnet. Many installations only have access to their local devices but not switches in other subnets or the router that bridges the subnets. Using this checkbox, the scanner gets the MAC address from the SNMP of the switch. This only works for switches.

## Device Configure - Links

Delete this text and replace it with your own content. While logged in, click on a device and on the side bar click the 'Edit' button on top. On the side bar go down to this section. Click "Save Changes" to preserve changes.



There may be up to eighteen Web Link if URLs have been associated with the current device under device info by the administrator.

When the device changes, the Links for a device also changes (to the ones having a context for that side view).

In the **URL Name** column enter what you want users to see when they click on a device under Device Info.

In the **URL External** box enter the link to the page a view will see.

There are two types of links that can be put in the URL External box: a URL to a local or remote web page, or a file (e.g. pdf).

If the file is on the IntraVUE™ host computer, enter the the relative path to the file starting at IntraVUE™'s web browser home directory: We recommend this placeholder :c:\intravue\AutoIP\tomcat8\webapps\ROOT

Copy or move the documents you want to add as links anywhere in or below this folder. Feel free to create new folders. Do NOT create a folder named 'doc' under ROOT, that is a reserved folder name. In the example above, the Floor Layout is stored at

c:\intravue\AutoIP\tomcat8\webapps\ROOT\manuals\LocationLayout.pdf

and the URL is entered using forward slashes instead of back slashes as shown below.

/manuals/samples/LocationLayout.pdf

If a HTML document contains image files be sure to move them also. (You may have to create additional folders to store images that are referenced by the HTML file in relative paths.)

The other type of link is to a page on a different computer. As long as the users browsing to the IntraVUE™ host also have access to the other remote computer, you can link documents on other computers. In this case, enter the full URL to the linked page including the http:// .

NOTE: Filenames are case sensitive, check the case if the link does not seem to work.

### **Links to other IntraVUE™ Hosts**

There is a setting in the ivserver.properties file that controls the link that is sent to the email recipient. This establishes the IntraVUE™ View that will be used and whether icons and thumbnails should be on or off when the IntraVUE™ browser page opens. See the end of the file.

This setting can be superseded by settings in the URL used to browse to IntraVUE™. The weblink below will open the IntraVUE™ browser on the 10.2.3.44 computer in Location View with Icons off and Thumbnails on. Uppercase I and T set Icons and Thumbnails on, lowercase i and t set them off. The view numbers are defined in the ivserver.properties file.

http://10.2.3.44:8765/iv2/ivue.jsp?v=3iT

This is particularly helpful when using the IntraVUE™ Supervisor edition.

## Configure Menu

## Configure Menu - Registration

Registration Scanner Plant Layout **BETA** Database Email General Advanced

REGISTRATION

Your registration has been completed

LICENSE TYPE

Enterprise

LICENSE SIZE  
(NODES DISCOVERED / NODE LIMIT)

83 / 2048

KEYCODE

PRODUCT KEY

✓

SERVICE CONTRACT

REGISTRATION CODE

To get your registration code click [here](#).

Submit Registration

The top section of this tab will provide registration information including...

Registration Status: Successful or Unsuccessful

License Type: Enterprise, Trial, Demo

License Size: Nodes Discovered Vs. Node Limit

Expiration Date: This is when your scanner completely stops

Keycode: This is required at the time of license registration

Product Key: You license Available from your purchase order or support contract

Service Co

which IntraVUE™ version is installed, how many nodes have been found and how many nodes IntraVUE™ is licensed for.

## Configure Menu - Database Tab

IntraVUE™ preserves the entire discovered topology and device properties in a database (\*.dmp). You can delete, restore, or export this database with the available options below.

Database   Email   General   Advanced

---

**Main Database Options**

**DATABASE CONFIGURATION**

**Export Database**

**Multi-Device Properties Export/Import**

Auto-backup   Clear   Restore   Backup   Export/Import   Archive

BACKUP LOCATION  
C:\INTRAVUE\DBBACKUP\AUTOBACKUPS

ENABLE AUTOMATIC HISTORICAL BACKUPS  
☒

BACKUP FREQUENCY  
Daily

NUMBER TO KEEP  
12

Apply

### Auto-backup

The "Enable Automatic Historical Backups" option provide a series of regular backups without further user actions. You may schedule the automatic backups to be done on a daily, weekly, or monthly basis. Whichever interval you select, you can also set how many of these backups will be kept.



The time of the first backup is loosely based on when automatic backups is enabled and then will be on 24 hour intervals after that. There is not a control to set the time of backup at this

time. Once the number of backups has been reached, the oldest backup is deleted after a new backup.

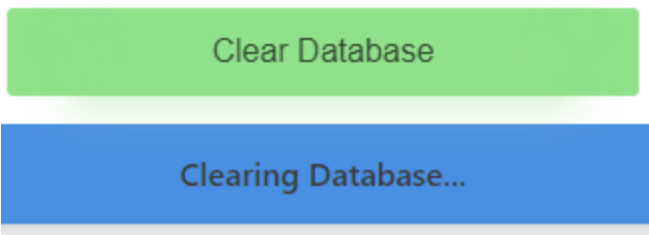
Make sure to click "Apply" after changing anything in this configuration.

## Clear

Deletes the entire database first and then restores IntraVUE™ to a blank database containing no networks configured.

The option "Keep Current Email Settings After Clear" preserves your email configuration and device email configuration after clearing the database.

When clearing a database you will get as status message just like the one below.



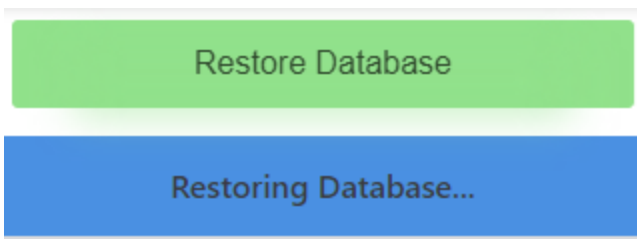
## Restore

Applies a new database from file while replacing the existing database.



A restore does a clear first, so you do not need to manually do a clear before restoring a database

When restoring a database you will get as status message just like the one below.





### Keep Current Email Settings

The option "Keep Current Email Settings " preserves your email and device email configuration from the present database, and ignores the one from the restored database.

### Keep IntraVUE Scanner Offline After Database Restore

Check this whenever you want to load a new database without active scanning to it (e.g. the scanner does not make changes to the database like moving or deleting devices).

To restore a database:

1. Click on the Restore button
2. Click on the \*.dmp file you want to restore (if viewing offline see [View Databases Off-line](#)).
3. Once the \*.dmp file is highlighted, click "Restore Database". Wait for confirmation message.



If you selected Off-Line mode and would like the scanner to start actively scanning again, restore the database one more time and don't select this option.

## Backup

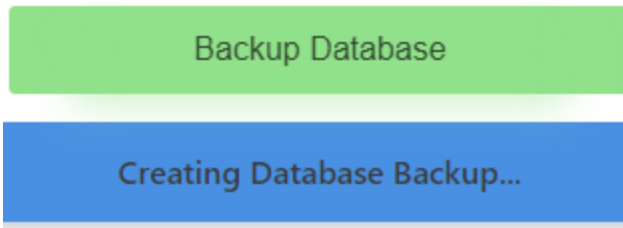
Backup allows a user to make a backup of the currently used database (\*.dmp). This is useful when a problem occurs in the network and you want to preserve as much data as possible with the 3-6 hour threshold resolution.

To create a backup simply provide a Database File name and click "Backup Database"



It is not necessary to stop IntraVUE™ for any of these operations.

When restoring a database you will get as status message just like the one below.



## Export/Import

See [Export / Import](#)

## Archive

See [Generate Support Archive](#)

## Configure Menu - Scanner Tab

The Scanner Tab allows you to configure networks and IP Address scan ranges so you can select the devices you want to monitor with IntraVUE™.

NETWORK NAME	USE LOCAL COMPUTER	TOP PARENT	SCAN RANGE	AGENT NETWORK	NET GR
VLAN 1	<input checked="" type="checkbox"/>	192.168.174.1	192.168.174.1		

Remove Network

Add Range

Add Network

### Admin Verify All Devices

At the top is a button that conveniently allows you to which have not yet been Admin Verified. This is provided as a alternative to configuring each device individually. See [Admin Verification in IntraVUE 3](#) for the benefits of Admin Verification.

## Scan Settings

### SNMP Read Community

At the top of the scanner tab you set the default SNMP community, if you are not familiar with SNMP you could think of this as a password. This community is used for devices which have not been otherwise configured with a community. Note that IntraVUE™ only reads SNMP information and never writes SNMP data.

A device is only updated with community information after successfully establishing SNMP communication. From then on it can only be changed in the Device Configuration dialog. This field should always be set to 'public' unless you are trying to discover switches or devices that use something else. You can enter special communities for switches and once the switches have been discovered with that, you can put it back to 'public' and let newly discovered devices get found using 'public'.

### Multiple SNMP Communities

The SNMP community for a device will not be set until successful SNMP communication to that device. You may set the default to the value of the switches and let all the switches be learned and then set it to another community and then those device communities will be set - all without using Device Configure. At the end we recommend leaving the community set at 'public', the SNMP default, which will apply to most newly discovered devices.

## Scan Speed

The speed of the IntraVUE™ scan engine can be conveniently adjusted with the Scan Speed dropdown listbox. IntraVUE™ 3 has made major improvements in the scan engine where in most cases you can run the scanner at the "Slow" speed (safest) and still be fast enough to map and monitor large networks. However, you can select from available speeds, if you think your network switches can allow the ARP rate without causing disruptions.

# of Devices	Speed	ARP Request Rate
Less than 150	Slow	60 millisecond gap between each outgoing packet and a limit of 20 unknown devices/ARPs per scan cycle
151 - 600	Medium	15 millisecond gap between each outgoing packet and a limit of 64 unknown devices/ARPs per scan cycle
601 - 1300	Fast	4 millisecond gap and a limit of 64 unknown devices/ARPs.
1300+	Ultra	1 millisecond gap and a limit of 64 unknown devices/ARPs.  This is okay as long as there are no old PLCs (e.g. PLC5).



**Alert:** Some very old Ethernet devices, e.g. PCL 5/40, may misbehave or reset when using Fast or Ultra scanner speed settings when not using the recommended setting, or when other scanning software is running in parallel on the same automation network. Check with Panduit

IntraVUE Support to learn more before attempting to increase Scanner speed above the "Medium" value.

## Device Configuration

### Reset Plant Layout

Resets the position of all nodes in the Plant Layout view back to the default position set by the scanner.

## Network Configuration

Three buttons allow you to **Add**, **Edit**, or **Delete** networks.

*Removing a network or removing devices from a scan range deletes all devices in that network . Previously deleting did not delete the devices from the IntraVUE™ database. If you want to remove all traces of ALL networks, use the Clear Database button in the Database Tab.*

### Add Network

Selecting the Add button displays the Network Add Dialog. If you have VLANs, [Virtual Local Area Networks](#), you should review [VLANs - Virtual Local Area Networks](#)

When you Add or Edit a network you can assign the network a name. Network names must be unique. Note: you can not change the top parent of a network once it has been configured.

### Add the Top Parent

The **Use Local Computer** checkbox is a convenience for using one of the local computer's network interfaces as the top parent. The local computer should be the top parent in 90% of the cases. See [Selecting The Top Parent](#) for details. When checked, a drop down list contains the IP Addresses of all the network cards of the local computer, normally just one. If you see the IP Address 0.0.0.0, there is a NIC card that is disabled or not connected in the host's network configuration.

If you uncheck this checkbox, you can enter the IP Address of a router. A router is the only other device which can be a top parent. The top parent is the device which has the ARP table for the devices MAC address to be correctly mapped to their respective IP addresses.

When the Top Parent IP address is entered the Scan Range will be automatically populated as a Class C host address range as calculated by a using netmask 255.255.255.0.

### **Add Range**

Once you have selected the top parent, use the Add button in the Scan Ranges group to add additional IP Address ranges until all the devices you want to monitor have been added.

A scan range may be as little as one device by entering the same IP as the starting and ending address. This is done to add specific switches, routers, or devices to a scan range.

*Example: Scan only 10.1.1.100*

*Starting IP Address 10.1.1.100*

*Ending IP Address 10.1.1.100*

*Example: Skip 10.1.1.100*

*Starting IP Address 10.1.1.0*

*Ending IP Address 10.1.1.99*

*Example: Skip 10.1.1.1-10.1.1.100*

*Starting IP Address 10.1.1.101*

*Ending IP Address 10.1.1.255*

### **Add IntraVUE Agent**

If you are using the IntraVUE™ Agent for this network, check the 'Use Agent' checkbox and additional fields will be available.

NETWORK NAME	TOP PARENT	SCAN RANGE		AGENT NETWORK
PLCs	10.132.58.170	192.168.1.1	192.168.1.254	<input checked="" type="checkbox"/>
	<button>Remove Network</button>	10.132.58.170	10.132.58.170	X
		<div>Add Range</div>		

(Pick the Agent's IP Address which can be pinged from the IntraVUE™ Host, not the Agent's IP Address in the scan range of devices to be scanned by that Agent.)

As you enter the local IP address of the Agent in the Top Parent field you will see your values repeated in the '**AGENT IP ADDRESS**' field. Normally, the agent will be 'top parent' for the devices it will be scanning. If you need a router to be the top parent of the network, change the top parent's IP Address' to be that.

For any IntraVUE™ network that will have ip addresses that are duplicates of the ip addresses in other similar networks, a unique '**AGENT NETWORK NET GROUP NUMBER**' must be assigned. The Net Group number count starts at zero and gradually increases as you add additional networks marked as agents.



You may also use the Net Group number of 0 to handle certain cases (e.g. no SNMP access to layer 3 switches)

See also [Completing Initial Configuration](#)

### Devices Not Correctly Positioned



**Note:** If your computer has multiple NIC cards, each NIC should be the top parent of its IntraVUE™ network. If the switches for an IntraVUE™ network you are scanning are in a different network segment/VLAN, be sure to add those switches to the scan range so devices may be discovered at their correct positions.

## Configure Menu - Email Tab

1. Open a browser and go to <http://127.0.0.1:8765>. Change 127.0.0.1 to the address of the remote IntraVUE host as necessary.
2. Click Configure to access the system menu and click on the “Email” tab.
3. Check the 'Enable Email' checkbox to activate email alarms.



Note that on a new scan checking this checkbox will not result in ANY emails being sent. That is because, by default, no device will have its 'Send Email to Default User' checked (See **Settings Required on Device Configuration** Below).



### EMAIL CONFIGURATION

Enable Email:



SECONDS TO WAIT FOR ALARM TO CLEAR BEFORE SENDING:

30

EMAIL ADDRESS TO SEND ALARMS TO:

control.engineer@myCompany.com

REPLY-TO ADDRESS IN EMAILS:

control.engineer@myCompany.com

EMAIL SERVER:

smtp.somewhere.com

SMTP PORT NUMBER:

25

Enable SMTP Authentication:



SMTP USERNAME:

jwmName

SMTP PASSWORD:

serverPassword

Enable Encryption:



Test Email

Apply

- The "SECONDS TO WAIT FOR ALARM TO CLEAR BEFORE SENDING" box sets the number of seconds an email alarm will be delayed before transmission. At the end of the delay

time, IntraVUE will check to see if the alarm condition is still valid. If it is, the email will be sent at that time. 30 seconds is the default setting.

5. The "EMAIL ADDRESS TO SEND ALARMS TO" box field is the email address that will receive the email alarms for all devices. If there are more than one recipient you want to send emails alarms to separate each email address with a comma (e.g. user1@company.com, user2@company.com, etc).
6. The "REPLY-TO ADDRESS IN EMAILS" box is required when your SMTP server requires a valid email address when emails are bounced back. It is also the reply to address that will be on the alarm emails (i.e. the "From" field). This email address may or may not have to be valid depending on your SMTP server.
7. The "EMAIL SERVER" requires the mail STMP server that will relay emails from IntraVUE™ to the email(s) on step 5 above.
8. The "SMTP PORT NUMBER" is necessary to connect to the SMTP server that will be relaying the email. Port 25 is the common.



It's best to use a company SMTP server as public SMTP servers (e.g. gmail or yahoo mail) could take a long time to receive alerts.

9. SMTP Authentication and Encryption are optional and not required by IntraVUE to sent alerts.
10. The "Test Email" button will will immediately generate a test email using the settings entered in the earlier steps. If you make a change, select the APPLY button before selecting "Test Email". This feature avoids having to disconnect a device just to test your email settings.

### Settings Required on Device Configuration

In the [Device Configure - General](#), click 'Edit', 'Send Alarms' button. This is NOT enabled by default. If enabled the default user (specified under Configure > Email) will get email alerts for this device.

There is also an 'Send Alarms to Default User' button. If you want an additional email sent to someone besides the default user, click this button AND edit the 'Alarm Email Address' field for the email of the person to get email alerts for this particular device.

SEND ALARMS

ALARM EMAIL ADDRESS

nightshift@myCompany.com

x

SEND ALARMS TO DEFAULT USER

When the "Test Email" button does not work

When you use the Test Email button and you do not receive an answer, there will be some text in an Exception message indicating the specific cause of the failure. For instance refused by SMTP host, invalid user name or password, etc.

This message is found in the scanner log file located at ...\\intravue\\log and will be the ivserver\_(date)\_(time).out file at the time you pressed Test Email.

<p>A sample of what is generated. It was generated by doing a Test Email with the default Email Setup dialog. The stacktrace line "javax.mail.MessagingException: Unknown SMTP host: smtp.p.somewhere.com;" tells you that the SMTP host, the email service provider, is incorrect or that you can not connect to it.</p>	<p>0120 100016 event: Device 10.1.1.67 reconnected 0120 100054 event: Device 10.1.1.90 moved from 10.1.1.244:9 to 10.1.1.16:2 0120 100054 event: deleted child node at 10.1.1.244:9 0120 100111 event: 10.1.1.32 Ping Response Threshold Exceeded 0120 100122 received mod request send test email 0 0 0120 100122 send test email 0120 100123 EmailTask runs: Intravue has been instructed by the admin to send a test email. Please see http://10.1.1.59:8765/ to [unused] 0120 100123 Unexpected Exception thrown - stack-trace follows: javax.mail.MessagingException: Unknown SMTP host: smtp.somewhere.com; nested exception is: java.net.UnknownHostException: smtp.somewhere.com at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:1211) at com.sun-mail.smtp.SMTPTransport.protocolConnect (SMTPTransport.java:311) at javax.mail.Service.connect (Service.java:233) at javax.mail.Service.connect(Ser-</p>
---	---

```

vice.java:134) at javax.mail.Service.connect(Service.java:86)
at com.sun.mail.smtp.SMTPTransport.connect(SMTPTransport.java:144) at javax.mail.Transport.send0(Transport.java:150) at javax.mail.Transport.send
(Transport.java:80) at database.EmailTask.run(EmailTask.java:76) at java.util.TimerThread.mainLoop(Unknown Source)
at java.util.TimerThread.run(Unknown Source) 0120 100146
device 10.1.1.67 disconnected 0120 100146 event: Device
10.1.1.67 disconnected 0120 100207 device 10.1.1.90 reconnected

```

## Email Alarm Types

IntraVUE™ will generate an email alarms for the following events:

- » Device x.x.x.x disconnected - See [Event Log Descriptions](#)
  - » Subject: "Intravue alarm ip=w.x.y.z"
  - » Body: "Intravue reports device w.x.y.z has disconnected. Please see IntraVUE™ Link"
- » Device x.x.x.x reconnected - See [Event Log Descriptions](#)
  - » Subject: "Intravue alarm ip=w.x.y.z"
  - » Body: "Intravue reports device w.x.y.z has reconnected. Please see IntraVUE™ Link"

## Customizing the Email Message

The email message that is sent to the user can be customized. See [The ivserver.properties File](#).

- » The email subject line can be customized to include the device name.
- » The email body for a device disconnected message can add the device name and link.
- » The ip address used to provide a link to the IntraVUE host can be changed to allow users requiring a proxy address rather than the real host address to reach the IntraVUE browser.

### **Configuring SMS Notifications**

IntraVUE can send SMS notifications to phones that already have SMS notifications configured whenever they receive an email. This forwarding mechanism allows the phone carrier or third-party to forward every email or specific emails to be sent to a cellular phone in SMS format. We recommend contacting your cellular carrier or email provider on how to enable email forwarding to SMS for your cell phone.

## Configure Menu - General Tab

### GENERAL CONFIGURATION

USER DEFINED 1 VIEW NAME:

User Defined 1

USER DEFINED 2 VIEW NAME:

User Defined 2

USER DEFINED 3 VIEW NAME:

User Defined 3

LABEL FIRST LINE OF TEXT:

IP Address

LABEL SECOND LINE OF TEXT:

Device Name

LABEL THIRD LINE OF TEXT:

Vendor

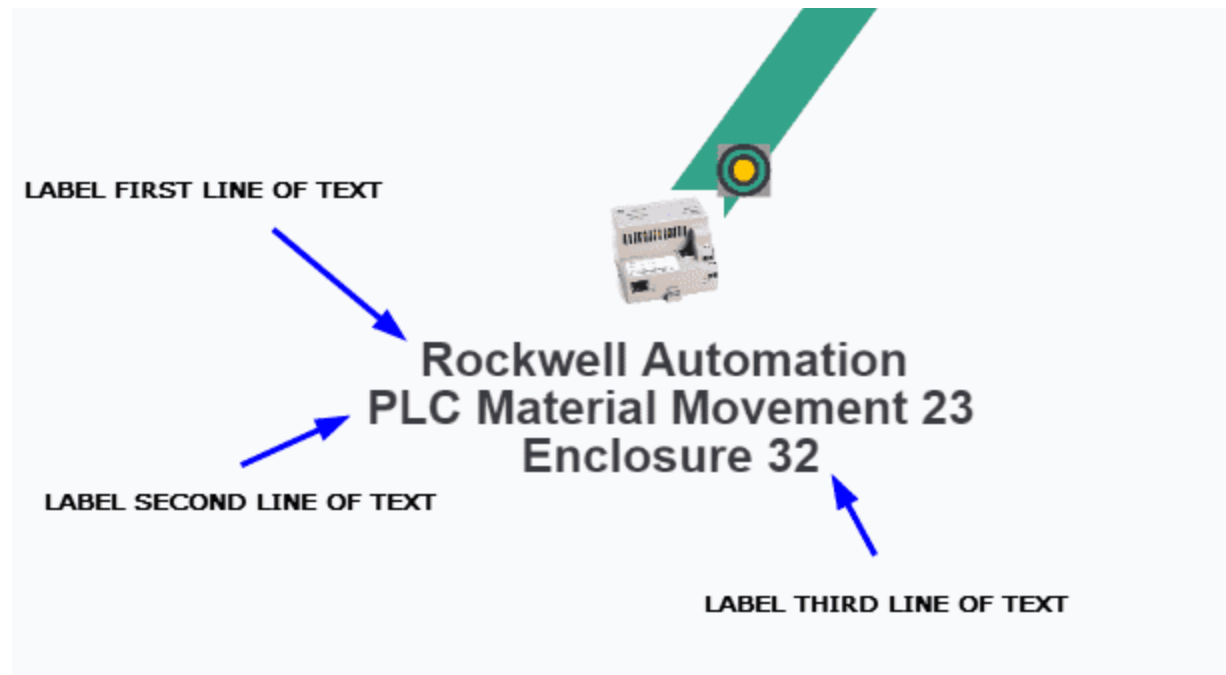
Apply

The first three boxes allow you to change the title for the first User Defined fields(1,2, and 3) available to every device. The title you set here will appear anywhere that particular User Defined field is used (e.g. Device List). See [Device Configure - Other Names](#) to modify the values of each of these fields. The next three User Defined fields (4, 5, and 6) are commonly known as Revision, Vendor, and Model. These are automatically obtained and hence there are no User Defined fields for them here. See [User Defined Fields](#) also.

### Device Name Labels

IntraVUE™ 3 replaced the concept of views with device labels. This new functionality allows the end user see multiple name labels under each device rather than having to click and change the view constantly.

The bottom three define which name labels are automatically placed under each device by the scanning process.



You can change the name labels by picking each line of text from the dropdown options including:

The **Device name** label is the SNMP device name or NetBios name if these are available.

The **IP Address** label is always the IP Address.

The **Location** label is the SNMP location information if SNMP is available from the device.

The User Defined 1 field. See [User Defined Fields](#)

The User Defined 2 field. See [User Defined Fields](#)

The User Defined 3 field. See [User Defined Fields](#)

---

There is a setting in the `ivserver.properties` file that establishes the default IntraVUE label that will be used when the browser is initially launched. See [The ivserver.properties File](#)

---

## Configure Menu - Advanced Tab

[Database](#) [Email](#) [General](#) [Advanced](#)

ADVANCED CONFIGURATION

Thresholds

Remove Ghost Nodes

Archive

Defaults

Adjust Ping Thresholds

DEFAULT INITIAL THRESHOLD LEVELS

PING RESPONSE TIME THRESHOLD (MSEC)

30.0

PING FAILURE THRESHOLD (%)

20.0

TRANSMIT BANDWIDTH THRESHOLD (%)

30.0

RECEIVE BANDWIDTH THRESHOLD (%)

30.0

### Thresholds

The default threshold values for all links are below. We recommend you check with the automation equipment manufacturer about what is the recommend threshold setting for their network interface. These are the most commonly used values in industrial automation environments.

Transmitted Bandwidth Threshold (30%) - Maximum percentage of available bandwidth used for transmitting.



Received Bandwidth Threshold (30%) - Maximum percent of available bandwidth used for receiving.

Ping Response Time (30 msec) - Maximum response time to a ping request from the IntraVUE™ host to the device.

Ping Failure Threshold (20%) - Minimum percentage of failed pings in a one-minute period.

See [IntraVUE Diagnostics](#) & [IntraVUE Analytics](#) to learn the more about the effects of exceeding these values.

### Adjust Ping Thresholds

Many links might simply have long response times (e.g. Wi-Fi, RF, unintelligent or old devices, poor cabling) and this will create a lot of "Ping Response Threshold Exceeded" events even when the device at the end of the other side of the link would still be functioning normally.

IntraVUE™ allows you to automatically increase the ping response time threshold value for all links that have exceeded their ping response threshold setting in the last 2 hours. When you click "Adjust" IntraVUE™ will set the new default ping response time threshold value to be 10 msec above their highest ping response time threshold value in the last 2 hours.

Once IntraVUE™ has automatically increased the default ping response time threshold for all affected links a "Request Successful" message will appear on this page. Additionally, you can go to the Events tab and look for a message similar to "auto-adjusted ping threshold for device x.x.x.x to 870 msec" where x.x.x.x is the IP address of the device which ping response time threshold was automatically increased.

### Remove Ghost Nodes

This feature allows you to remove all ghost nodes at once without having to delete each ghost node individually. Simply go to the Configure menu > Advanced > Remove Ghost Nodes, and click "Remove Ghost Nodes". Once you get the confirmation message go back to "View" and you will notice that all ghost nodes were removed. See [Admin Verification in IntraVUE 3](#) to learn more about why ghost nodes are created.

### Active Directory

An IntraVUE™ administrator can set up Active Directory authentication as an additional security layer. By using Active Directory authentication, the default admin account for IntraVUE™ will be disabled. This will result in requiring all users having to log on to IntraVUE™ using an Active Directory account when they open IntraVUE™.



Before you enable AD for IntraVUE™ work with your IT department to get the required information below:

- » Active Directory URL
- » UserBase
- » GroupBase
- » Service Account Username
- » Service Account Password
- » Admin Group
- » Read Only Group

### **Active Directory Server Setup**

1. Enter the AD Server settings. Click "Next".
  1. Active Directory URL: IP of the AD server
  2. Active Directory User Base: This is the folder location of the users in AD.
  3. Active Directory Group Base: This is the folder location of the groups in AD.



Active Directory URL: This can be an AD server with authentication only, or authentication + encryption (e.g. TLS)

### ADVANCED CONFIGURATION

Thresholds	Remove Ghost Nodes	Active Directory
------------	--------------------	------------------

Enter the information below to configure IntraVUE to use Active Directory to authenticate users. Note that using Active Directory will disable the default admin account and will require all users to log into IntraVUE.

ACTIVE DIRECTORY URL

10.132.56.100:389

ACTIVE DIRECTORY USER BASE

CN=Users,DC=iot-demo,DC=com

ACTIVE DIRECTORY GROUP BASE

CN=Users,DC=iot-demo,DC=com

Next

2. Enter the AD credentials for IntraVUE™ to authenticate to the AD server. Click "Next".
  1. Service Account Username: This would be an account used to query the AD server and make sure the connection is valid, the AD configuration for IntraVUE™ is correct, and to validate the Admin and Read-only groups in AD.
  2. IntraVUE™ Admin and Read-Only Groups: Enter the names of the groups from AD and assign to either admin or read-only role here. These groups should have existent AD users in them before adding them here.

## ADVANCED CONFIGURATION

Thresholds	Remove Ghost Nodes	Active Directory
------------	--------------------	------------------

Enter the information below to configure IntraVUE to use Active Directory to authenticate users. Note that using Active Directory will disable the default admin account and will require all users to log into IntraVUE.

SERVICE ACCOUNT USERNAME

administrator@iot-demo.com

SERVICE ACCOUNT PASSWORD

.....

INTRAVUE ADMIN GROUP

IntraVue-Admins

INTRAVUE READ-ONLY GROUP

IntraVue-Readonly

Previous

Next

3. Add a post-login banner of your choice. Click "Next".



According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a login banner decreases the chance of intrusion by twenty percent.

### ADVANCED CONFIGURATION

Thresholds	Remove Ghost Nodes	Active Directory
------------	--------------------	------------------

Check the box below to show a dialog box after a successful Active Directory login. The text in the textbox below will be the content of the dialog box shown to the user. The user will need to acknowledge the dialog box in order to gain access to IntraVUE.

SHOW POST-LOGIN DIALOG



```
*****WARNING*****
You are entering a private internet area. It is for authorized use only. By using this system, all users
acknowledge notice of, and agree to comply with, the security policies of this company. By continuing to use
this system you indicate your awareness of the terms and conditions of use.
LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.
*****
```

Previous

Next

4. Select an encryption type or none to simply authenticate to an AD server. Click "Apply".
  1. **SSL**<sup>1</sup>. Requires you to apply a security certificate
  2. **STARTTLS**<sup>2</sup>. Requires you to apply a security certificate

---

<sup>1</sup>SSL and TLS are cryptographic protocols, both provide a way to encrypt communication channel between two machines over the Internet (e.g. client computer and a server). SSL stands for Secure Sockets Layer and current version is 3.0. TLS stands for Transport Layer Security and the current version is 1.2. TLS is the successor to SSL. The terms SSL and TLS can be used interchangeably, unless you're referring to a specific protocol version. The ordering of protocols is: SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2.

<sup>2</sup>STARTTLS is a protocol command, that is issued by an email client. It indicates, that the client wants to upgrade existing, insecure connection to a secure connection using SSL/TLS cryptographic protocol. STARTTLS command name is used by SMTP and IMAP protocols, whereas POP3 protocol uses STLS as the command name. Despite having TLS in the name, STARTTLS doesn't mean TLS will be used. Both SSL and TLS are acceptable protocols for securing the communication.

## ADVANCED CONFIGURATION

Thresholds	Remove Ghost Nodes	Active Directory
------------	--------------------	------------------

Select the type of encryption. If an encryption is selected, the certificate for the Active Directory server will need to be uploaded.

ENCRYPTION TYPE

STARTTLS

CERTIFICATE

 ldapCert

5. You will get a login prompt screen from this point onward everytime you try to connect to IntraVUE™



## IntraVUE

USERNAME

intravue-admin@iot-demo.com

PASSWORD

.....|

## Admin Verification in IntraVUE 3

Admin Verification is a process of establishing a controlled state of your network, or the devices which you are monitoring with IntraVUE.

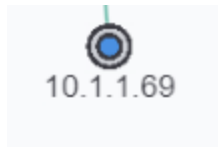


Rogue devices can be easily identified when all devices have been previously verified (see below) and when using device filters (see [View Filters](#))



Refer to [IntraVUE Legend](#) to understand node fill, outlines, and connecting line colors.

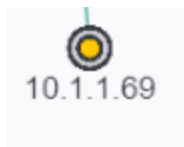
Each Admin Verified node has additional characteristics from a non-Verified node.



The node is normally blue filled.



If the position of the device changes the originally verified position becomes red filled.



The new position of the device becomes a tan filled node.



If the device that moved comes back to the original location, the tan filled node will go away and the red filled node will become blue filled again.



Failure to admin verify all of detected devices by IntraVUE will result in incomplete Analytics & KPIs Status Reports, missing configuration of newly detected devices, inability to detect when a device has moved or disconnected from ring or linear networks, and impairs your ability to identify what assets truly belong to your plant network and troubleshoot them accordingly.

When a node is tan filled it will stand out. It will call your attention to it. Find out what it is and then verify it or take some action to get the device off line.

A second tan filled node is the 'ghost' of the real position of a device. The real device will have a real IP name like 1.100.56 and the ghost node will have the IP 10-1-100-56.

If you see a tan filled node, find the corresponding tan filled node with dashes in the IP address.

If the new position is acceptable, delete the ghost tan filled node and admin verify the new position.

In the future this two step process will become one step.

If the position is temporary, you may leave the red filled ghost. When the device is returned to its former position the red ghost will be replaced by a blue filled node.

To make Admin Verification easy, there is a single button that will automatically verify every device with an IP address that has not yet been verified. It's on the Scanner Tab of the [Configure Menu - Scanner Tab](#). See also [Device Configure - General](#) for verifying individual nodes.



## Adding Users and Changing Admin Password

### Normal Login

Admin Login is accessed from the System Menu by right clicking in the background of the browser interface.

When you are logged in as administrator additional options are available in the System Menu and Device Menu.

There will be black outline surrounding the browser window when you are logged in as the administrator.

In IntraVUE™, the default admin password for IntraVUE™ is the same as the admin password for the Apache Tomcat Manager, intravue.

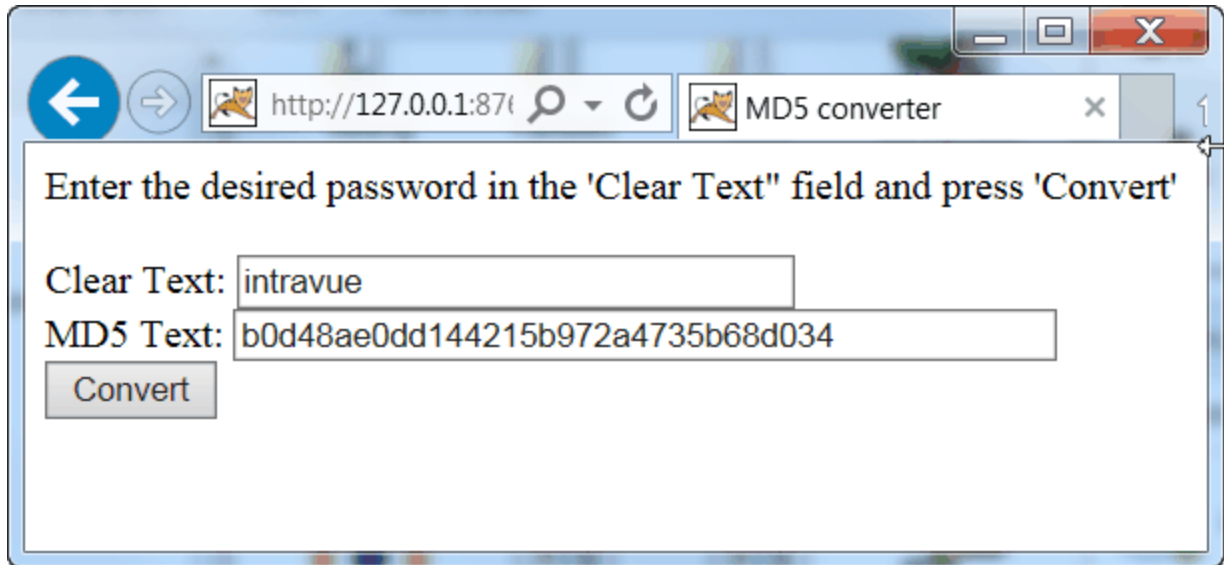
### Changing the Admin Password

The password is set in a file in the IntraVUE™ installation folder ...\\IntraVUE™\\AutoIP\\tomcat8\\conf, named tomcat-users.xml. Find the XML tag that starts with "user" and contains a username of "admin". The password entry is the password for both the tomcat manager and IntraVUE™, as shown below. The text after password, in quotes, is the MD5 hash of the plain text password, in this case "intravue".

```
<user username="admin" password="b0d48ae0dd144215b972a4735b68d034" roles-  
s="admin,manager"/>
```

The MD5 hash is a method of making the password secure should someone be able to open the tomcat-users.xml file.

To create an MD5 hash of the password of your choice go to this URL <http://127.0.0.1:8765/tools/md5.jsp>



In the image above you can see intravue was added as the Clear Text password and after the Convert button was selected the MD5 text was created. The MD5 text returned is what you want to insert in the password=" " parameter in the tomcat-users.xml file.



**Change the password from the default of "intravue" after registering your IntraVUE software to prevent unauthorized personnel from gaining admin level privileges in IntraVUE.**



**Failure to limit access to the IntraVUE™ host can allow unauthorized personnel modify the tomcat-users.xml file.**

With IntraVUE™'s remote administration capabilities, there is no need to have physical access to the host computer. The directories where security information is configured are not accessible from the web interface. See [Accessing IntraVUE™ remotely via any Internet Browser](#) to require all users to remotely connect to IntraVUE without having to be on the IntraVUE host.

### **Adding Username and Password Protection to the IntraVUE™ application**

The Apache Tomcat web server that provides the user interface for IntraVUE™ can be configured to require a username and password before a user can see the IntraVUE™ web page.

The first step is to add security data to the file ...\\intravue\\AutoIP\\tomcat8\\webapps\\iv3\\WEB-INF\\web.xml. Copy the lines below and insert them at the end of the file, just before the closing </web-app> line.

```
<!-- Define a Security Constraint on this Application -->

<security-constraint>

<web-resource-collection>

<web-resource-name>Intravue Application</web-resource-name>

<url-pattern>/*</url-pattern>

</web-resource-collection>

<auth-constraint>

<!-- NOTE: This role is not present in the default users file -->

<role-name>intravue</role-name>

</auth-constraint>

</security-constraint>

<!-- Define the Login Configuration for this Application -->

<login-config>

<auth-method>BASIC</auth-method>

<realm-name>Intravue Application</realm-name>

</login-config>

<!-- Security roles referenced by this web application -->

<security-role>

<description> The role that is required to log in to the IntraVUE™ Application </description>

<role-name>intravue</role-name>

</security-role>

</web-app> NOTE: do not copy this line. Insert just before this line in the file
```

The above will require the user to login as the 'role-name' intravue. Role-names are defined in the file tomcat-users.xml, described above. The role 'intravue' is already defined in that file and has a user-name of IntraVUE™ and a password of intravue.



**If you are going through this process then you really want security that anyone reading this help file will not be able to break.**

Therefore, you should edit the tomcat-users.xml file and add a new role. The two line below can be added to this file and will create a new role named 'remote' and this role will have a username of remoteUser and a password of intravue2

```
<role rolename="remote"/>
```

```
<user username="remoteUser" password="intravue2" roles="remote"/>
```

To complete the process edit the data in the lines in the sample above and change the lines starting with to have the role 'remote' rather than 'intravue'. Then restart the Windows service "Apache Tomcat eTomcat".

Anyone logging in will now be required to use a username and password to login.



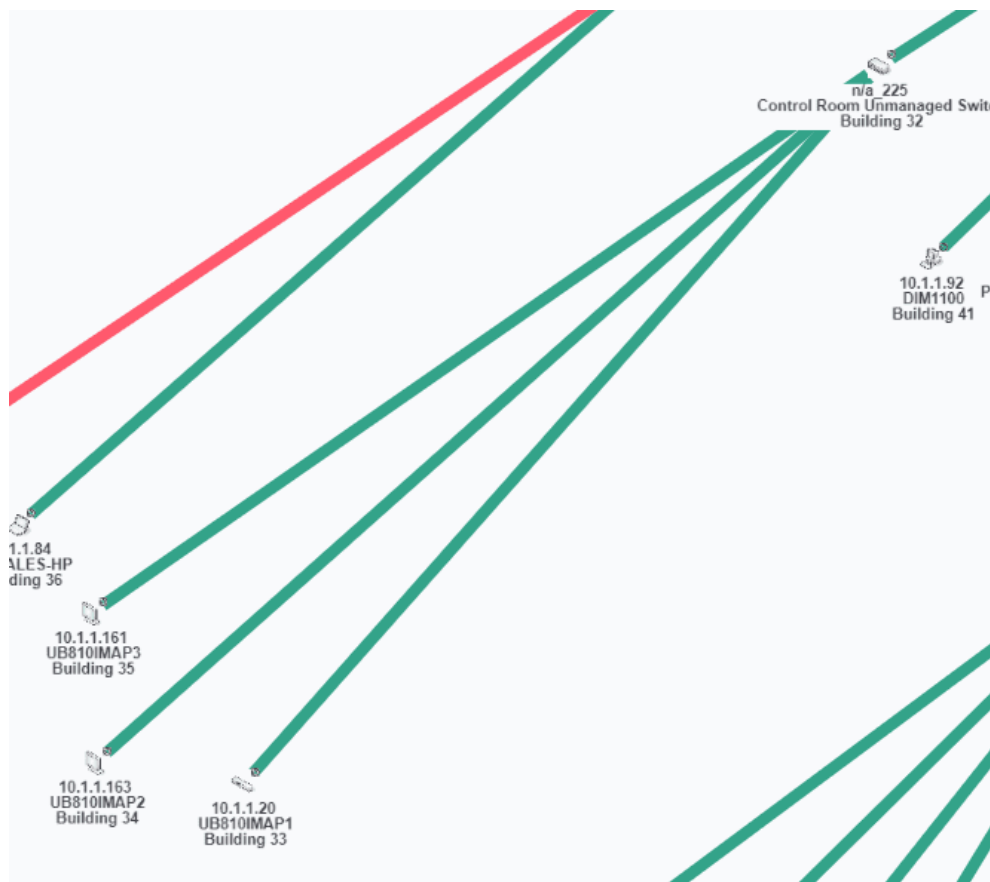
**Note:** You may create as many username and password combinations for the role remote as you like by adding additional <user.. lines to the tomcat-users.xml file.

## VM Host, Hub, or Non-SNMP Switch

### Unmanaged and Web Managed Switches

An unmanaged switch that has an IP address but which does not support SNMP will be found and displayed under an auto-inserted node along with the devices that are directly connected to the switch. This is because they will all be found on the same port of the unmanaged switch's parent and any lower down managed switches will see them on the 'uplink' port back toward the IntraVUE™ host.

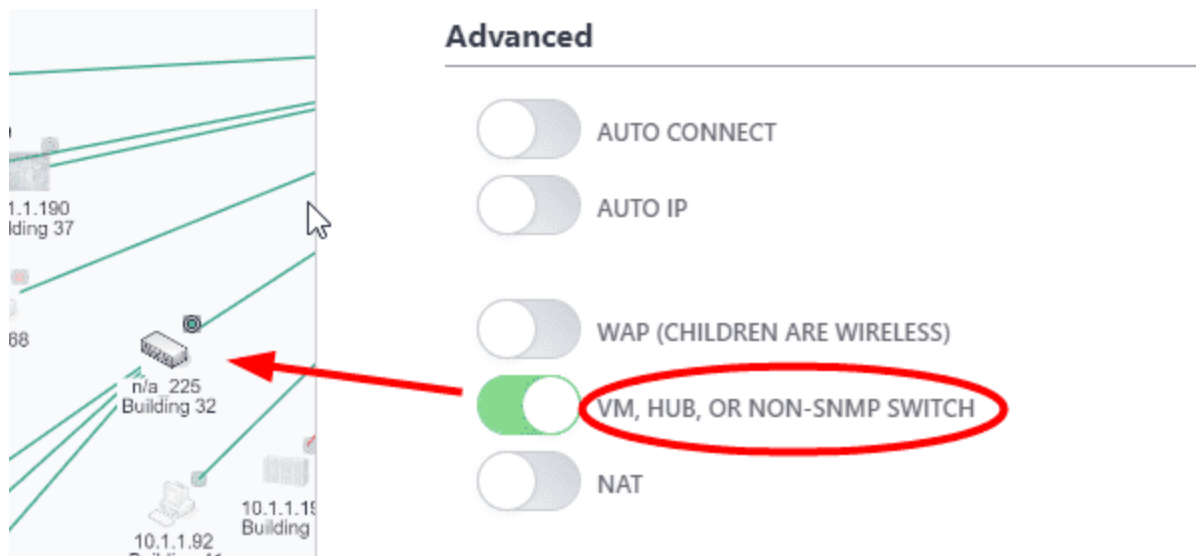
The image below shows the way IntraVUE™ will display an unmanaged switch that has an IP address having two devices connected to it. If a managed switch does not have its SNMP community set correctly it will appear the same. The 10.1.1.20 device is an unmanaged switch with the .161 and .162 devices physically attached.



The parent managed switch of these devices reports them all on the same port, so IntraVUE™ automatically inserts a node, labeled 'n/a' to represent the hub or unmanaged switch which must be present.

To learn the difference between 'n/a' nodes and 'N/A' nodes see [NA Nodes](#) for more details.

In order to show the network as it physically exists the administrator can select the Configure item from the unmanaged switches Device Menu. Check the checkbox 'Unmanaged Switch or Wireless AP' or 'Virtual Machine, Web Managed Switch, Access Point' on newer IntraVUE versions. Click 'Apply and Close'.



After a minute, the auto inserted node will go away as there is now only one device on the port of the managed switch and the other two devices are below it.



Some old unmanaged switches and hubs don't have a IP address by default or because of missing configuration. IntraVUE will not be able to see these without an IP address. In order to show the network as it physically exists you can add child nodes and move attached devices under this unmanaged switch. This is not recommended as monitoring for that switch is very limited.

## Virtual Machines

Similar to unmanaged switches, a virtual hosts server will display an 'n/a' node with devices physically attached to it. In order to show the network as it physically exists the administrator can select the 'Configure' item from the virtual machine's Device Menu. Check 'VM, HUB, or NON-SNMP SWITCH' and then Click 'Apply and Close'. After a minute, the auto inserted node will go away as there is now only one device as the virtual host and the other devices are below it.

## Utility Programs

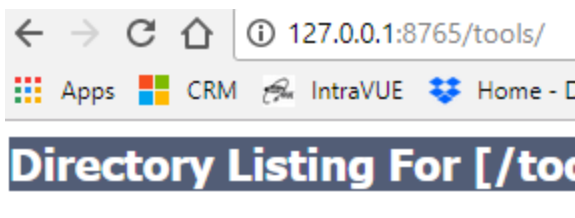
### Tools Folder

With the introduction of the IntraVUE PLUG, several utilities have been added which are available for all versions of IntraVUE.

To see what is available use the URL below in your IntraVUE browser, substitute the URL of IntraVUE for the 127.0.0.1.

<http://127.0.0.1:8765/tools> - HTTP

<https://127.0.0.1:8766/tools/> - HTTPS



#### Filename

[agentconfig\\_all.jar](#)

[archiveclient.jar](#)

[date.jsp](#)

[firefox/](#)

[ivd.war](#)

[md5.jsp](#)

[putty/](#)

[snmpx.war](#)

[super.war](#)

[superkpi.war](#)

[switchprobe.jar](#)

[util.jsp](#)

[winscp/](#)



- **archiveclient.jar** - selecting this link will over to download/save the jar file on the computer you are browsing from. By saving this file on a remote computer, you can easily create a batch file which saves the .zzz file created by the Generate Support Archive item on the main menu.

- **date.jsp** - clicking on this item will allow you to change the date and time in the IntraVUE Plug. This utility is specific to the IntraVUE Plug ONLY. Normally you would set the IntraVUE Plug to gets its time from an NIST time server, however, if this is not possible you can change the appropriate fields on this page to set the date and time.

### SwitchProbe

- **switchprobe.jar** - brings up the java version of this utility or you can open it from Windows Start button > programs > intravue / tools / run switchprobe menu item. See also Downloads, and [Verifying SNMP on Fully Managed Switches](#)

The Switchprobe utility can also collect Q-Mib data in addition to the Bridge Mib

The syntax hint must be added to the URL you use to access IntraVUE. For instance, if you access IntraVUE using "http://10.1.2.3:8765" the full URL for each of the utilities above would be:

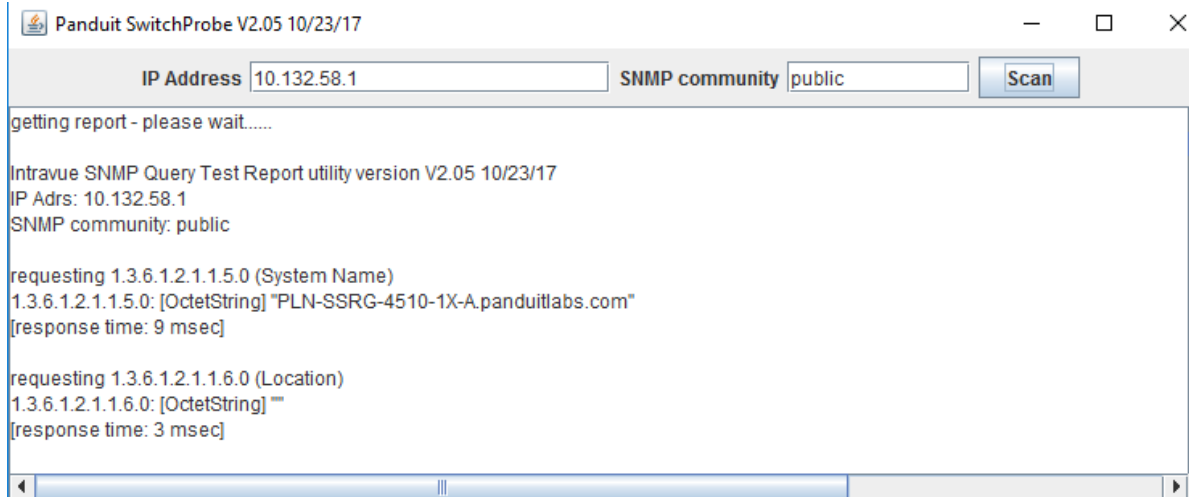
http://10.1.2.3:8765/tools/util.jsp?ping=10.1.2.99

http://10.1.2.3:8765/tools/util.jsp?tracert=10.1.2.99

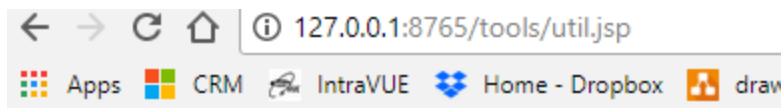
http://10.1.2.3:8765/tools/util.jsp?switchprobe=10.1.2.99&community=public

This utility is available on the IntraVUE Agent and the regular IntraVUE software. After you run one of the commands, a browser window will open with the results of running the utility.

The switchprobe option is nice if you want to use the browser's find command to locate specific data within the switchprobe results.



• **util.jsp**- If you select this page you will get a list of available utilities with their syntax hints. More utilities will be added over time.



```
echo usage:
tools/util.jsp?ping=1.2.3.4
tools/util.jsp?tracert=1.2.3.4
tools/util.jsp?switchprobe=1.2.3.4&community=public
```

# User Defined Fields

IntraVUE provides 6 user defined fields available to each device found. There are user defined fields for which the name can be configured by the administrator (see [Device Configure - Other Names](#)). The main user interface and other dialogs make use of these names entered in the General Tab. Until changed by the admin they have these name values:

**User Defined 1 = "Customizable field"**

**User Defined 2 = "Customizable field"**

**User Defined 3 = "Customizable field"**

**User Defined 4 = %"Revision obtained by scanner%"**

**User Defined 5 = %"Vendor obtained by scanner%"**

**User Defined 6 = %"Model obtained by scanner%"**

## Server

## IntraVUE File System

## Predispose.txt File

IntraVUE™ has a mechanism to set all SNMP configuration upon the initial scan so the end users can prevent SNMP discovery on certain devices even before the initial scan.

The “predispose.txt” suppresses SNMP properties through an SNMP.suppress code based on mac or IP address of the device. Each line identifies a device by either its IP address or MAC address. A range of MAC addresses can also be used. A netgroup is not required but IntraVUE™ acknowledges each line as network 0.

To see SNMP.suppress codes see [CSV Column Values](#)



Any errors (e.g. typos or strange characters) on any lines on this file will cause the entire predispose.txt logic to fail

### Examples

Ignore SNMP Device Name (8) and Ignore SNMP Location (4).

**ip 10.1.2.3 SNMP.suppress = 12**

Ignore SNMP Bridge Mib data

**mac 12:34:56:00:00:00 to 12:34:56:ff:ff:ff SNMP.suppress = 2**



Predispose.txt file can be edited directly from <http://127.0.0.1:8765/plug/admin/editfile.html>. Just like the trunkingdef.txt file the predispose.txt file will survive an upgrade

# The IntraVUE folder

## Organization

The directory in which IntraVUE™ was installed contains the following folders:

- **Autoip** - contains IntraVUE components including the web server used by IntraVUE.
- **CleanDbBackup** - files for creating a clean database. It also contains a batch file to create a clean database without a browser.
- **dbBackup** - storage of user created saved databases and automatically created databases
- **dbBackup\timedBackups** - storage for one minute resolution backups when setting is enabled in ivserver.properties. See [The ivserver.properties File](#)
- **intravue\_install** - installer log
- **Log** - folder for detailed internal logging
- **Plant Layout** - sample plant layouts
- **Tools** - utility programs.

The Autoip folder contains many files. Those of interest to a user/administrator of IntraVUE are:

- **bootpdata.xml** - The XML equivalent of the optional AutoIP user interface. The data is stored in this file.
- **ivserver.properties** - contains settings not normally changed by users. Details are found at ivserver.properties.
- **ivserver.properties.new** - IntraVUE upgrades do not overwrite the current file, instead the upgrade defaults are stored here. Any new items a user would like to use need to be copied to the ivserver.properties file before they can be used.
- **ivserver.xml** - contains settings and configuration for SNMP data and the Modbus/TCP Server. Details are found at ivserver.xml.
- **scanner.log** - a log of all bootp and dhcp requests seen by autoip and any responses made by AutoIP.
- **trapmailer.xml** - a configuration file for interpreting traps sent to the IntraVUE host and redirecting the traps to an email server. Details within the file.

- **predispose.txt** - contains the IPs or MACs of devices that do not need to be included in SNMP scanning. See [Predispose.txt File](#)

The 'tomcat8' folder under autoip contains all the files for the Apache Tomcat web server. This is used by IntraVUE™ to provide a user interface to the IntraVUE™ database. The only folder of interest to users is the ROOT folder of the web server. The ROOT folder can be accessed from any computer browsing to the IntraVUE™ web server. Users are free to create their own content below this folder, including creating new folders. The path to the ROOT folder is:

...\intravue\autoip\tomcat8\webapps\ROOT



# Backing up files not in the MySQL database backup file

When you make a backup from the System Menu or System Config dialog, you are backing up the MySQL database that contains all the data used by IntraVUE. This backup does not contain any content referenced by IntraVUE.

In the event of a catastrophe, installing a new copy of IntraVUE from the installation CD and then restoring a saved backup will get you to where you were at the time of the backup. Content added by the user will not be in the backup.

Other files that could be backed up via the Windows' backup application or by scheduled tasks might include:

- User created content
- User modifications to IntraVUE default files.

The mescaline data files are typically located on hard disk on which IntraVUE was installed, in the c:\mysql\data folder. This entire folder and its subfolders **MUST BE EXCLUDED** from any backup software as well as any antivirus software. When the mysql database becomes large, these programs will lock critical resources longer than mysql can withstand. The result will be that the mysql service stops and consequently the IntraVUE™ scanner will not be able to make any updates until the mysql service is restarted via reboot or by the user.

User created content can only be in the web server root folder described above. All user created content is preserved during upgrades. Backup the entire root folder to save any content you have added.

## The ivserver.properties File

This file is located in the autoip folder of IntraVUE, normally ...\\program files\\intravue\\autoip ( ).

Each of the parameters that can be set in this file contains a description of the parameter and a sample line showing the default value. These are shown as comment lines in the file. THE FILE IS MEANT TO BE SELF DOCUMENTING.

Comment lines start with a '#' character and have no effect.

This file typically contains configuration items that are not normally changed by IntraVUE users or administrators. It is usually only changed after consultation with IntraVUE Technical Support.

Open the file with notepad or wordpad to view the various options or to make changes.

Note: When upgrading to new versions of IntraVUE, this file will be updated for any NEW configuration items. Any settings already applied will not be changed. The new items will be set to their default states.

A configurable zoom value for the Start screen is navigable in **Topology View**.

### **session.backuptimerbackups**

5 - Five backups each having the last six hours with one minute resolution data guaranteeing you have access to 24 hours worth of one minute data

### **view.settings**

Sets the default first label for each device.

# Special Files in IntraVUE

Most configuration data is stored in the mysql database. There are some additional files that also contain configuration data. User modifications to IntraVUE default files would only be contained in one of the following files, all in the c:\program files\intravue\autoip\ folder:

bootpdata.xml

ivserver.properties

ivserver.xml

trapmailer.xml

trunkingdefs.txt

Name	Size	Type
htdocs		File Folder
instext		File Folder
scripts		File Folder
tomcat5		File Folder
abootpd.jar	105 KB	Executable Jar File
activation.jar	54 KB	Executable Jar File
autoip.err	0 KB	ERR File
autoip.out	1 KB	OUT File
autoip-service.exe	64 KB	Application
bootpddata.xml	1 KB	XML Document
daemon.exe	68 KB	Application
ivnvi.dll	28 KB	Application Extension
IVServer.err	0 KB	ERR File
ivserver.exe	64 KB	Application
ivserver.jar	284 KB	Executable Jar File
IVServer.out	0 KB	OUT File
ivserver.properties	4 KB	PROPERTIES File
ivserver.properties.new	4 KB	NEW File
ivserver.xml	2 KB	XML Document
mail.jar	340 KB	Executable Jar File
mysql-connector-java-3.0.14-...	232 KB	Executable Jar File
probeautoip.bat	1 KB	MS-DOS Batch File
TrapMailer.err	1 KB	ERR File
trapmailer.exe	64 KB	Application
trapmailer.jar	76 KB	Executable Jar File
TrapMailer.out	1 KB	OUT File
trapmailer.xml	9 KB	XML Document
uninstallautoip.exe	37 KB	Application
uninstalltomcat.exe	37 KB	Application
uninstalltextsvcs.exe	33 KB	Application
uninstallIVServer.exe	37 KB	Application
uninstallTrapMailer.exe	37 KB	Application

**bootpddata.xml** contains the configuration data for the optional AutoIP program. Data in this file normally comes from the AutoIP user interface, the Device Configuration's 'Enable Autoip' checkbox, or by directly editing this XML file. Note that checking the Enable Autoip checkbox will cause an entry to be added to this file, but unchecking it will not cause it to be removed. You can only remove an entry using the AutoIP user interface or editing this file in a text editor.

**ivserver.properties** contains fine tuning parameters for the scan engine as well as some user interface enhancements that are not yet part of the browser based user interface. Each parameter is preceded by an explanation using the comment # sign at the start of each line. The line starting without a # sign is the actual parameter in use.

Note that when an upgrade is installed, the original `ivserver.properties` file is updated for any NEW settings, any existing settings are not changed. The `ivserver.properties.new` file contains the default settings for all options, it is not used by Intravue.

**ivserver.xml** contains configuration data for the Modbus/TCP interface as well as extra SNMP data that is displayed on a device's 'SNMP Data ...' menu item. Follow the link for more details.

**trapmailer.xml** provides extended functionality for getting and sending information about trap messages. All configuration is done in this file which is also self documenting in the form of comments.

Note: the full capabilities of trapmailer are complex and require an effort to understand.

## Modbus - TCP and SNMP Data Configuration

IntraVUE provides connection and SNMP information through an embedded Modbus/TCP server on the default Modbus port, 502.

Additionally, all configured SNMP data is visible in the IntraVUE browser by selecting the SNMP Data... item from the Device Menu.

The information to be provided is configured in the file "ivserver.xml", which is located in the ...\\intravue\\autoip folder (file system details) .

IntraVUE makes information available to HMI and SCADA devices in the same way they would access information in a PLC. ivServer can also be configured to provide any SNMP variables through the Modbus/TCP interface.

The file starts and ends with a dataserver line.

```
<dataserver mysql="127.0.0.1">
```

```
.....
```

```
</dataserver>
```

There are three other types of lines in the ivServer.xml file, located between the above two lines..

## Ping or Connection status

Lines that start with "ping" create Modbus/TCP registers for the current connection status of a device.

Note: Register 0 in the ivserver.xml file is the first 40000 or 4X register in Modbus which has an offset of 1 and which is actually register 4:0001.

```
<ping reg="0" ip="192.168.100.2" />
```

```
<ping reg="10" ip="10.1.1.45" />
```

In the above example, the ping status of the device 192.168.100.2 will be stored in the 0th or first Modbus 4X register. This is generally referred to as 4:00001 or 400001. The ping status of 10.1.1.45 will be stored in Modbus register 4:00011.

## Disabling Modbus TCP

Due to other software, it may sometimes be necessary to disable IntraVUE from acting as a modbus/tcp server. In these cases edit the `ivserver.properties` file and change the below value to be 'false'.

```
modbus.service=true
```



# Handling Trunking in Switches

Some switches can be configured to treat two or more ports as if they were a single port. One reason for doing this is to get more bandwidth between two switches. Another reason is the result of 'load balancing'.

IntraVUE asks a managed switch for the port number of the MAC devices connected to it. In the case of trunking, the response could be any of the ports used for trunking. As a result IntraVUE will see the 'lower' switch as moving frequently between the trunked ports, and the IntraVUE display will redraw each time there is such a change.

A configuration file has been created that allows the IntraVUE administrator to inform the scanner of any trunking for switches being scanned.

'trunkingdefs.txt' is the default file name. It is located in the ...\\intravue\\autoip folder (file system details ) . The actual name used is user configurable in the ivserver.properties file, in the property 'scanner.trunk.data.file'. An administrator could then setup several different trunking files for testing and other purposes.

A side benefit of using the 'trunkingdefs.txt' file is the ability to renumber ports to suit the users view of the switch, see Example 3 in [The 'trunkingdefs.txt' File](#).

## The 'trunkingdefs.txt' File

This file is read and interpreted to both combine ports for trunking purposes and also to change the port numbers assigned to a switch for display purposes. This is specially true for Cisco switches. The file is located in C:\intravue\autoip\trunkingdefs.txt

The format is simple. A switch is designated using square braces, [ ], around its IP address. This is followed by one or more lines of port assignments until the next set of square braces.

The port assignments are done using a two character separator "->". On the left is the port as known to the switch. On the right is how IntraVUE should treat and display that port.

Many ports on the left can be assigned to the same number on the right. If a number is repeated on the left, the last one will be used.

### Example 1 - Normal Case

The 10.1.2.3 switch has ports 2 and 3 trunked to ports 5 and 6 of switch 10.1.2.4. We want IntraVUE to consider ports 2 and 3 on the 10.1.2.3 to both be treated as port 2 and ports 5 and 6 on the other switch to be treated as port 5.

```
[10.1.2.3]
```

```
2->2
```

```
3->2
```

```
[10.1.2.4]
```

```
5->5
```

```
6->5
```

### Example 2 - Showing different port numbers for Stacked Switches

When two 24 port switches are stacked, the port numbers of the second switch are changed internally so they do not conflict with the first switch. On some switches the first port of the second switch might be numbered 25, or 27 if there are some internal ports, or even a high number like 950.

This example shows the second stacked 8 port switch that has been renumbered for display purposes.

```
[10.1.2.3]
```

10->1

11->2

12->3

13->4

14->5

15->6

16->7

17->8

### **Example 3 - A Switch with misnumbered ports**

In this example the label on a switch numbers the ports 1 thru 12, but internally the ports are 12 to 1. IntraVUE reports the port number used by the switch internally and this leads to confusion. A Cisco 2955 is an example of such a switch.

[10.1.2.3]

1->12

2->11

3->10

4->9

5->8

6->7

7->6

8->5

9->4

10->3

11->2

12->1

## Customizing the email message

The email message that is sent to the user can be customized using options in the `ivserver.properties` file.

- The email subject line can be customized to include the device name.
- The email body for a device disconnected message can add the device name and link.
- The ipaddress used to provide a link to the IntraVUE host can be changed to allow users requiring a proxy address rather than the real host address to reach the IntraVUE browser.

Contact [techsupport@panduit.com](mailto:techsupport@panduit.com) to get help on customizing the subject and body of the email

## VLANs - Virtual Local Area Networks

VLANs provide a means to group devices as if they were the only devices in a subnet.

VLANs are configured in Layer 2 switches.

Broadcast traffic within a VLAN is not broadcast to devices outside the VLAN even if they are attached to the same switch. This is one of the main advantages of a VLAN. It can shield devices from seeing the broadcast traffic of other devices, including ARPs.

If two devices are attached to the same layer 2 switch but they are in different VLANs, the physical traffic between the two devices must travel the path of the connected cables from the layer 2 switch thru any other switches until it reaches a router, which will then send the traffic back down the same wire to the original layer 2 switch. There the traffic will go to the port of the device on the other VLAN.

## How to Add an additional web server Port Number

IntraVUE uses port 8765 to view web pages and to communicate internally. Some users may desire a different port number due to proxy servers or when going through a firewall. IntraVUE can be configured to 'listen' on additional port numbers, but will ALWAYS listen on port 8765 which MUST be available for IntraVUE's use.

Below are the steps to configure the Tomcat web server to use port 80, as an example.

1. Make sure that port 80 is not in use already with some other web server (eg IIS, Apache) From a command line, do

```
netstat -an
```

You should NOT see a line like

```
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
```

If you do, you'll have to find out which web server is using that port and stop it before continuing. Look down the services list and see if there's anything like httpd, apache, IIS, ... The other web server must be configured to use another port or must not run to avoid a race for the port on restarts.

2. Using windows explorer, navigate to the directory C:\Program Files\IntraVUE\AutoIP\tomcat5\conf
3. Make a safety copy of the file server.xml by selecting it, then copy (Ctrl-C) and paste (Ctrl-V)
4. Open the file server.xml with notepad (it's a pretty short file - only about 30 lines long)
5. Add an additional line after the assignment to port 8765. YOU MUST NOT REMOVE THE 8765 LINE. So,

```
< Connector port="8765" / >
```

becomes

```
< Connector port="8765" / >
```

```
< Connector port="80" / >
```

6. In the services list , stop and then start the service 'Apache tomcat etomcat'
7. Confirm you can still talk to the IntraVUE server by pointing your browser at URL

`http://127.0.0.1:8765/iv2/list`

8. Confirm it ALSO works on the default port 80 by using URLs

`http://127.0.0.1:80/iv2/list`

`http://127.0.0.1/iv2/list`

9. You should now be able to see IntraVUE on port 80

`http://127.0.0.1`

Note that you cannot remove the port 8765 from the server.xml file, because some internal functions expect to find the server on that port. However, all the applets will use the same port as the original connection, so it should work fine through firewalls which block port 8765.

Although it is possible in principle to accommodate an existing web server on port 80 without stopping it, the procedures for doing this are much more complex, particularly if the goal is to drill through firewalls. I would suggest IntraVUE be installed on a dedicated machine to avoid these issues

## IntraVUE Logs

IntraVUE provides internal logs for advanced troubleshooting used by IntraVUE support. These are typically found under the C:\intravue\log folder as ivserver\_\*.out files.

### To Enable Verbose Logging

1. Go into C:\intravue\autoip\ivserver.properties
2. Search for 'debug.var=' which is the default value.
3. Change from the default value to 'debug.var=123456789' (the highest level of logging).  
IntraVUE Tech Support can help you with figuring out which level of logging is best.
4. Save the file and Close
5. Stop and restart the Auto-IP Server service from Windows services



Verbose logging can fill up your hard drive quickly. Be sure to disable verbose logging when not doing troubleshooting of IntraVUE.

To disable verbose logging:

1. Go back to C:\intravue\autoip\ivserver.properties
2. Remove the extra numbers from 'debug.var='. Save file and close.
3. Stop and restart the Auto-IP Server service from Windows services

### Log File Name Pattern

IntraVUE .out logs have the file name pattern as ivserver\_YearMonthDay\_timestamp.out. You can change the file name pattern to be something else by going into the ivserver.properties modifying the following setting:

```
log.file.pattern=../log/ivserver_$1.out
```

### Log File Rotation Size



IntraVUE automatically creates a new .out log file after 5000000 kb. You can change this to be smaller or large by changing this setting in the ivserver.properties file.

log.file.rotation.size=5000000 (Default)

### Log File Number of Events

IntraVUE can also truncate the number of events it creates, There are 2 settings. Whether you increase or decrease these, the .out log files will show all specified number of events .

# limit the number of event log items of a single type per device retained

eventlog.perclass.limit=200 (Default)

# limit the number of event log items of a non-repetitive type per device retained

eventlog.perclass.longterm.limit=400 (Default)

## IntraVUE Appliance

## Using the IntraVUE Appliance as an Agent

The IntraVUE™ Appliance is used as a scanning Agent allowing IntraVUE™ to visualize and monitor IP devices not in the "local" plant network as the IntraVUE™ host.

This is the most common use of the IntraVUE appliance where it's simply configured with a static (or dynamic) IP address and allows the IntraVUE host to scan the edge devices on the private or isolated network and add them to the Map View as if they were in the local plant network. The IntraVUE agent does not require additional licensing.

The Scanner Agent was developed to handle several situations:

- to scan remote networks which do not have a router (e.g. VLANs).
- to scan remote, routed networks where IT will not provide the SNMP read-only community of the router,
- to scan multiple networks which utilize common IP addressing (i.e. the same IP addresses exist in each network) such as I/O or OEM Systems, or
- to acquire more accurate data from remote networks with long delays between IntraVUE and the devices (radio modems in mines),



After obtaining an appliance in the available formats from below, see

[IntraVUE Appliance Configuration](#) for exact steps on configuring an IntraVUE™ Appliance as an Agent or Server.

### IntraVUE™ Appliance Formats

- A standard Panduit IntraVUE™ OEM part (WNMS-APPL) with standard 15/20amp outlet. This is the de facto IntraVUE™ Appliance hardware for many years and it is still sold as a Panduit product. See the Panduit Catalog [here](#) for more info.



- An Industrial Raspberry Pi (RPI) Agent: It comes with all certifications required for industrial use. It can be powered using 24v current and can be din railed mounted onto a cabinet. It also comes with the standard 15/20 amp power outlet when purchasing a standard power cord (optional). This is a third-party part number that can be purchased from the third-party distributor [here](#). It requires a Micro SD card (16GB) to load the IntraVUE™ Appliance Linux operating system that the Raspberry Pi motherboard will be using. See [IntraVUE Agent - Low Cost Agent](#) for configuration instructions and image download for this IntraVUE™ agent version.



- A DIY version allows you to have the versatility and benefits of the RPI IntraVUE™ agent but it requires assembly and does not come with all of the industrial certifications of the Industrial RPI Agent. See [IntraVUE Agent - Low Cost Agent](#) for assembly instructions, how to obtain the parts, and loading the OS image and IntraVUE™ software.

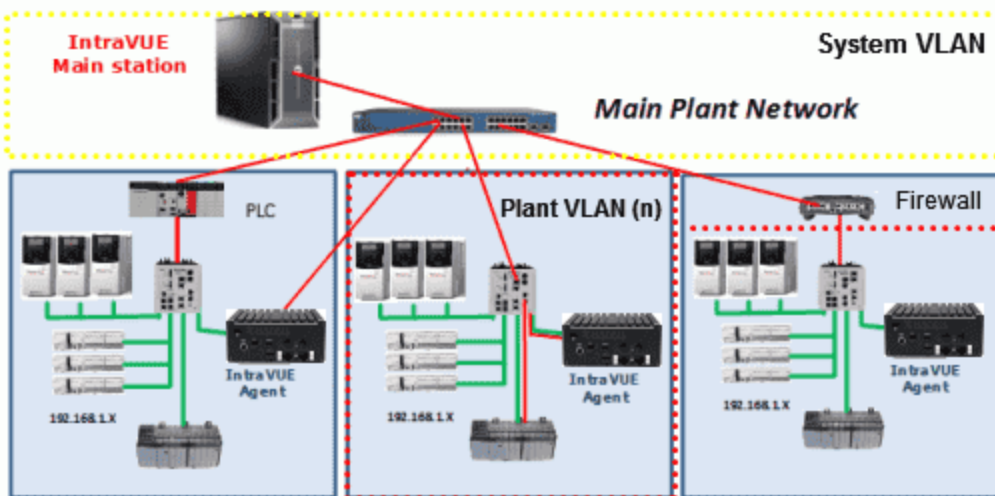


- A IntraVUE™ Appliance OVF for VMWare: This is a pre-configured virtualized linux-based IntraVUE™ ready to be deployed on any plant or isolated network. Simply download and install the available OVF image from the [OVF Image Download Page](#) and deploy on your local machine or virtualized environment.

The Agent performs local scanning of an isolated network and provides the results to the IntraVUE host computer. The ping and threshold data will be as if the Intravue host computer was located in the isolated network.

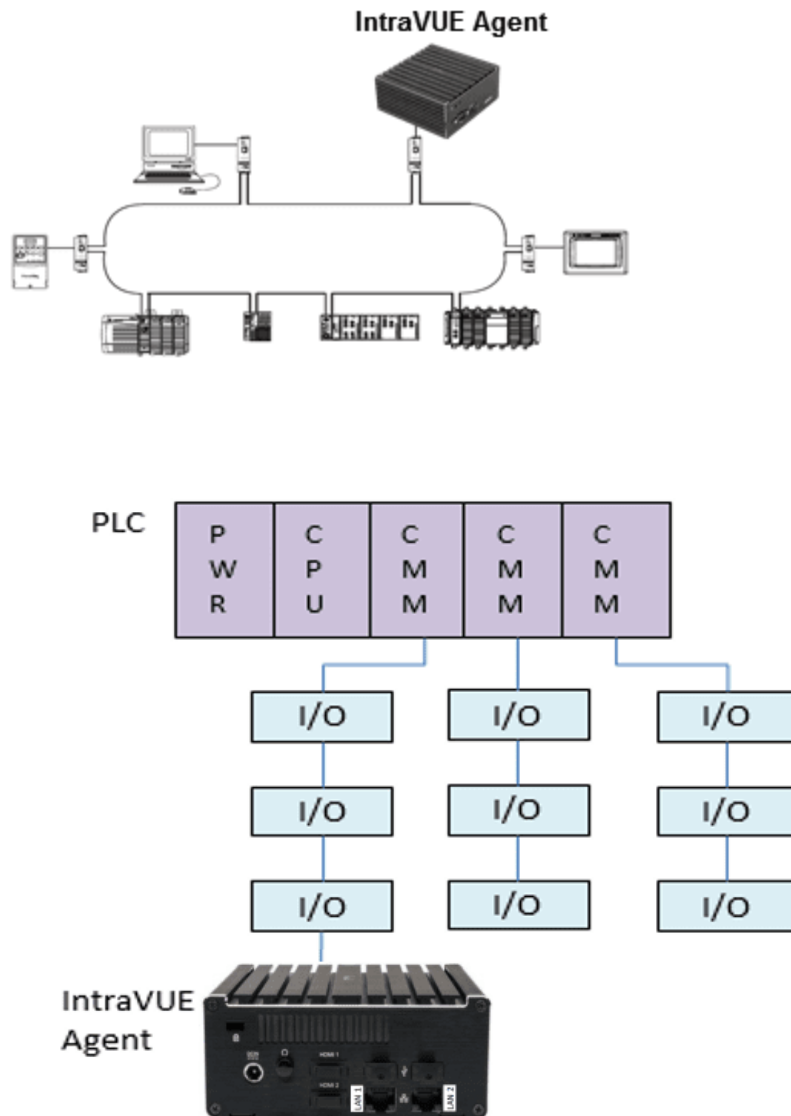
- Two independent Ethernet connections
- Two USB connections (when using the hardware appliance)
- 9 to 40 VDC input power (when using the hardware appliance)

IntraVUE Agents are easily configured with the IntraVUE to provide a complete Industrial Ethernet monitoring solution. Some OEM systems such as packaging machines or bottling machines contain their own private Ethernet networks. These systems typically use the same IP addresses for each function in the system. When you have multiple systems using the same IP addresses it is impossible to monitor networks inside the systems with traditional networking tools. IntraVUE Agents allow these multiple networks to be monitored by a single IntraVUE package.



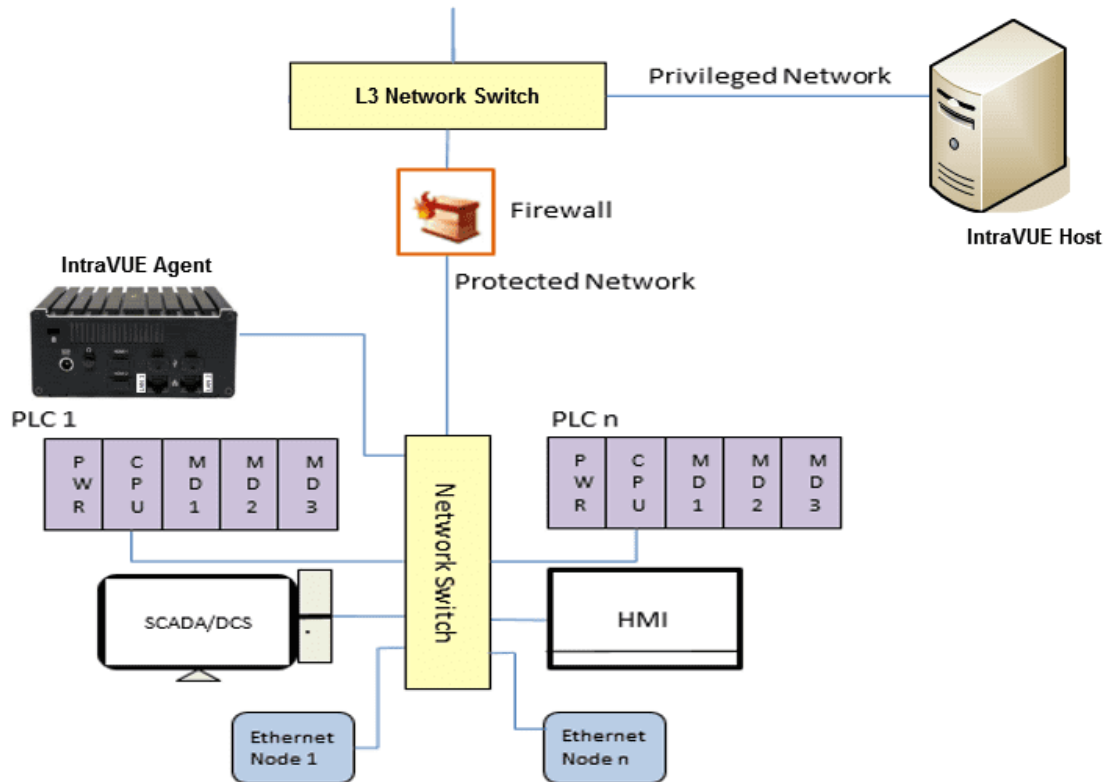
In the image above 3 different methods of connecting the IntraVUE Agent to the main IntraVUE workstation are shown.

PLC/DLR (Device Level Ring) Networks. The Agent is connected to a switch inside the 'system' using one port of the agent and the other port of the agent is connected to a switch on the 'plant' side.



VLAN Access. A switch within the 'system' is configured with 2 VLANs. One is the "Plant" VLAN of the 'system' and the other is the "PLC" VLAN that provides access from the plant to the PLC of the 'system'. The IntraVUE Agent has one interface connected to the switch on the Plant VLAN and the other agent's Ethernet interface connects to the PLC VLAN port on the same switch.

Firewall Access. Firewall device blocks all the traffic packets except from an IP address on the 'enterprise side' to the IntraVUE agent on the 'plant' side of the Firewall.



## Using the IntraVUE Appliance as a Server

The IntraVUE™ software act as a Server without the need for a host machine or virtual hypervisor (as in the case of the ovf Linux version image). The functionality and performance compared to a host machine does not very greatly and can be an option for many environments that are inclined to use IntraVUE™ in this format. You will need to have an the necessary hardware to act as an IntraVUE™ server.



See the necessary IntraVUE™ Appliance Hardware in [Using the IntraVUE Appliance as an Agent](#).



See [IntraVUE Architecture](#) to learn how the IntraVUE™ server works.



See [IntraVUE Appliance Configuration](#) for exact steps on configuring an IntraVUE™ Appliance as an Server.

### A. IntraVUE Appliance Port Configuration

Once the appliance is powered on and plugged to the core fully managed switch on the plant network, use the Intravue Plug Configurator as one of the ports must be appropriately configured for use as an IntraVUE Server.

### B. Accessing the IntraVUE Server

An IntraVUE™ Appliance comes with the full capabilities of the IntraVUE software. After the port configuration is done , you can access IntraVUE via a browser from any machine using the IP address of the IntraVUE host. This will look like `http://nnn.nnn.nnn.nnn:8765`. Log in as admin [default pw: intravue (case sensitive)]

You can also use the “Intravue Browser” button on the Intravue Plug Configurator, or opening an internet browser and entering the URL.



## IntraVUE Appliance Configuration



The IntraVUE™ appliance can be pre-configured to act as either a 1) server where no host machine is available to install IntraVUE™, or as an 2) agent bridging scanning to and from remote or isolated networks not local to the plant local network.

### Configuring the Appliance AS AN INTRAVUE AGENT

Configuration of an IntraVUE Appliance as an IntraVUE Server will enable you access non-routable networks.

STEP 1: Obtain the necessary IntraVUE appliance host	See <a href="#">Using the IntraVUE Appliance as an Agent</a> to learn more about the appliance formats.
STEP 2: Download the Plug Configurator (i.e. Discovery Tool)	Download the update package from the <a href="#">IntraVUE™ Support Page</a> . Go to downloads > "Download for Appliance/Agent/Plug" > Select the latest version "tools only" and extract all files. Open "agentconfig_all.jar"
STEP 3: Connect the Appliance to the physical network as an agent	Connect the appliance to the switch on the isolated network. Port LAN 1 (IP 1) should connect to a switch port accessible from the Plant Network (i.e. uplink). Port LAN 2 (IP 2) (downlink) should connect to a switch port that has access to the isolated network. Power up the unit.
STEP 4: Launch the Discovery tool and find the	<ol style="list-style-type: none"><li>1. Launch the Discovery tool</li><li>2. Find the Appliance on the plant network using one of these</li></ol>

nearest IntraVUE™ Appliance on the local plant network	<p>modes:</p> <ol style="list-style-type: none"> <li>1. <b>Broadcast:</b> Hit Update IP to for the Discovery tool to ping all devices in the local subnet.</li> <li>2. <b>Single IP address:</b> Enter the IP address of the appliance directly and hit "Update IP" to find the appliance.</li> <li>3. <b>Class C range:</b> Enter the IP of he network where there could potentially be IntraVUE™ appliances (e.g. 10.132.58.0).</li> </ol>
STEP 5: Configure the Ethernet Interfaces on the Appliance	<p>To configure an appliance you need to be in "Single IP mode" in the earlier step</p> <ol style="list-style-type: none"> <li>1. Click on one of the found appliance lines in the Discovery tool</li> <li>2. Select from either IP 1 or IP 2 depending which one has a non-zero IP address and click on "Adjust IP Parameters". Click 'OK' to accept the prompt.</li> <li>3. IP 1(uplink) is intended for bridging the plant network and so assign a static address (default is DHCP) and corresponding netmask.</li> <li>4. IP 2 (downlink) is intended for scanning the isolated network and so assign a static IP address (default 192.168.255.127) and corresponding netmask.</li> <li>5. Configure the default gateway. This would be the IP address of the router on the isolated network.</li> <li>6. Configure the DNS Server. This would be a DNS Server IP on the plant side of the network.</li> <li>7. Enter the password and hit 'Submit' to apply the changes. The appliance will reset and re-appear on the Discovery tool after a few minutes.</li> </ol>
STEP 6: Test connection to the newly	<p>To test access to the IntraVUE™ Agent:</p> <ol style="list-style-type: none"> <li>1. Click on the line that belongs to the target appliance on the Dis-</li> </ol>

<p>deployed IntraVUE™ Agent</p>	<p>covery Tool, select the correct IP 1/IP 2 port, and click "IntraVUE Browser". A browser windows will open with IntraVUE™.</p> <p>OR</p> <ol style="list-style-type: none"> <li>2. Open a browser interface on either the IntraVUE™ host or any machine on the local plant network. Change the URL to the IP of the IntraVUE™ host. This will look like <a href="http://nn.nnn.nnn.nnn:8765">http://nn.nnn.nnn.nnn:8765</a>.</li> <li>3. Click on 'Login' and log in as admin. Congratulations! Your IntraVUE™ Agent is ready to scan isolated networks.</li> </ol>
<p>STEP 7: Link the IntraVUE Agent to the IntraVUE™ Server</p>	<p>The configuration for an IntraVUE™ network using an Agent is very similar to a non-Agent network. Follow the First Scan steps in <a href="#">Completing Initial Configuration</a></p>

## Configuring the Appliance AS AN INTRAVUE SERVER

Configuration as an IntraVUE Server will enable complete functionality as a stand-alone instance of the IntraVUE System.

<p>STEP 1: Obtain the necessary IntraVUE appliance host</p>	<p>See <a href="#">Using the IntraVUE Appliance as an Agent</a> to learn more about the appliance formats.</p>
<p>STEP 2: Download the Plug Configurator (i.e. Discovery Tool)</p>	<p>Download the update package from the <a href="#">IntraVUE™ Support Page</a>. Go to downloads &gt; "Download for Appliance/Agent/Plug" &gt; Select the latest version "tools only" and extract all files. Open "agentconfig_all.jar"</p>
<p>STEP 3: Connect the Appliance to the physical network as a server</p>	<p>Connect the appliance to the switch on the isolated network. LAN 1 port should connect to a switch port accessible from the Plant Network (i.e. uplink). Port LAN 2 (downlink) should connect to a switch port that has access to the isolated network. Power up the unit.</p>

	<p>Connect the appliance to the local manufacturing network. Connect Port LAN 2 (downlink) to a switch port that has access to and from the plant network. Only a single port is necessary, however to access the system remotely port LAN 2 can be connected to the WAN.</p>
<p>STEP 4: Launch the Discovery tool and find the nearest IntraVUE™ Appliance on the local plant network</p>	<ol style="list-style-type: none"><li>1. Launch the Discovery tool</li><li>2. Find the Appliance on the plant network using one of these modes:<ol style="list-style-type: none"><li>1. <b>Broadcast:</b> Hit Update IP to for the Discovery tool to ping all devices in the local subnet.</li><li>2. <b>Single IP address:</b> Enter the IP address of the appliance directly and hit "Update IP" to find the appliance.</li><li>3. <b>Class C range:</b> Enter the IP of he network where there could potentially be IntraVUE™ appliances (e.g. 10.132.58.0).</li></ol></li></ol>
<p>STEP 5: Configure the Ethernet Interfaces on the Appliance</p>	<p>To configure an appliance you need to be in "Single IP mode" in the earlier step</p> <p>Use the Discovery Tool to discover the Appliance on the network.</p> <ol style="list-style-type: none"><li>1. Click on one of the found appliance lines in the Discovery tool</li><li>2. Select from either IP 1 or IP 2 depending which one has a non-zero IP address and click on "Adjust IP Parameters". Click 'OK' to accept the prompt.</li><li>3. IP 1 (uplink) is intended for autodiscovery and ease of deployment and hence it is already checked with DHCP by default (recommended).</li></ol>

	<ol style="list-style-type: none"> <li>IP 2 (downlink) is intended for scanning the plant network and so assign a static IP address (default 192.168.255.127) and corresponding netmask.</li> <li>Configure the default gateway. This would be the IP address of the router in the plant network.</li> <li>Configure the DNS Server. This would be a DNS Server IP address of the plant network.</li> <li>Enter the password and hit 'Submit' to apply the changes. The appliance will reset and re-appear on the Discovery tool after a few minutes.</li> </ol>
STEP 6: Test connection to the newly deployed IntraVUE™ Server	<p>To test access to the IntraVUE™ Server:</p> <ol style="list-style-type: none"> <li>Click on the line that belongs to the found appliance on the Discovery Tool, select the correct IP 1/IP 2 port, and click "IntraVUE Browser". A browser windows will open with IntraVUE™.</li> </ol> <p>OR</p> <ol style="list-style-type: none"> <li>Open a browser interface on either the IntraVUE™ host or any machine on the local plant network. Change the URL to the IP of the IntraVUE™ host. This will look like <a href="http://nn.nnn.nnn.nnn:8765">http://nn.nnn.nnn.nnn:8765</a>.</li> <li>Click on 'Login' and log in as admin. Congratulations! Your IntraVUE™ Server is ready to scan isolated networks.</li> </ol>
STEP 7: Register the Server License	<p>Purchase appropriately sized license through an authorized Distributor.</p> <p>Follow the registration steps in the <a href="#">Installation &amp; Registration</a> section of help to register your Appliance as an IntraVUE™ Server.</p>

STEP 8: Configure IntraVUE to scan the local network

The IntraVUE Server is now installed and ready to scan the target network. This will be done in the same way as a traditional server-based installation of IntraVUE. See "First Scan" in the [Completing Initial Configuration](#) section of the IntraVUE™ help.



Do not assign IP addresses used by other devices in the scan range to either IP 1 or IP 2 when statically setting either of these. If your network is made up of static IP addresses this can cause IntraVUE to show lots of "change mac" messages and duplicate IP issues in your Analytics report. This could create potential lockups for some devices when they comeback online and do a duplicate IP check.



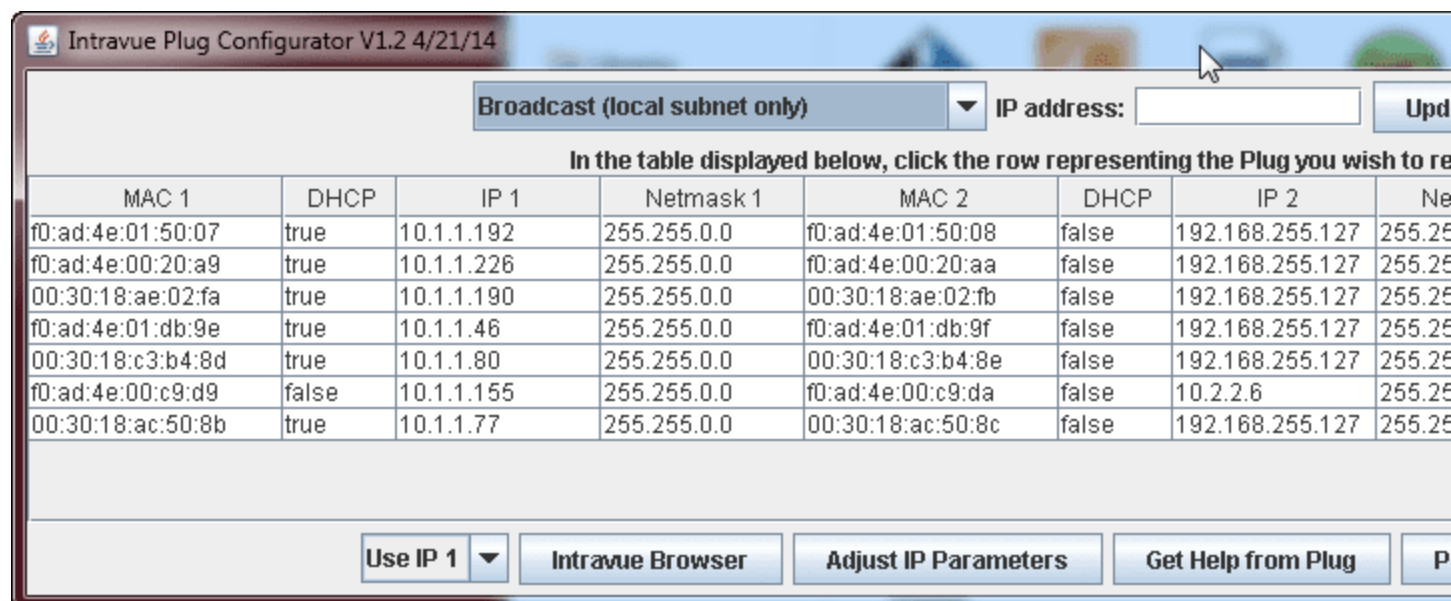
Antivirus software, firewalls or firewall rules, and windows group policies can prevent the discovery tool from finding an IntraVUE appliance (either placed as server or agent) even when connecting a laptop directly to the appliance. Make sure to disable these and try again using the discovery tool.

For Complete Configuration Instructions, refer to the [Appliance Quick Start](#)

## IntraVUE Discovery Tool

The IntraVUE™ Plug Configurator (a.k.a. Discovery Tool) is an advanced tool typically included with every IntraVUE™ installation.

The discoverytool utility uses broadcast traffic from a computer running the tool to communicate with and discover the appliance. Using broadcast traffic requires the computer and the appliance be in the same network/vlan. If VLANs are used and there are any switches between the appliance and the computer with the discovery tool, the ports carrying the traffic by all the switches involved must be in the same VLAN as the appliance and tool host.



The discovery tool is named agentconfi\_all.jar. This utility is available with every windows install by going to Start > Programs\Apps > IntraVUE. In the case of IntraVUE™ Appliances the discovery tool can be downloaded from [IntraVUE™ Support Page](#). Go to downloads > "Download for Appliance/Agent/Plug" > Select the latest version "tools only" and extract all files. Open "agentconfig\_all.jar"

### Accessing the appliance in networks having DHCP

The agentconfi\_all.jar utility uses broadcast traffic from the computer running the tool to communicate with and discover the appliance. If VLANs are used and there are any switches between

the appliance and the computer with the discovery tool, the ports used by all the switches involved must be in the same VLAN as the appliance and tool host.

The quickest and simplest method for connecting to and configuring an appliance that uses DHCP is to temporarily connect to and reconfigure the appliance

- The host running the discovery tool must be in the same subnet as the appliance.
- Connect Port LAN 1, the left port, to the network.
- The computer should NOT have any additional addresses in the same subnet as is being used, for example a wireless IP. If it does have a second address in the same subnet, disable that NIC during configuration.
- The appliance should also NOT have a second IP in the same subnet, even if the other port is not connected. This is the factory default condition.
- Launch the Discovery Tool in File Explorer by double clicking on agentconfi\_all.jar or by right clicking on the file and selecting Open. Note: Java is required on the computer running the discovery tool and must be in the path environmental variable.

If you launch the tool and nothing happens you probably do not have Java installed on the host computer. Check this in your Control Panel. If Java is not installed, go to <http://java.com> and download a 32-bit version of Java.

If you launch the tool and you see the column headings but no device is discovered, we recommend you follow the rules for connecting without DHCP (next section).

If DHCP is not available in the location where the appliance will be finally located, you can move the appliance into an office or other network which does have DHCP for purpose of configuration, and then move the appliance to its permanent location after configuration.

Alternatively, the appliance can be configured by configuring a computer to connect to the appliance using a fixed IP address:

- Configure the computer to have an IP address. The factory default fixed IP of the appliance LAN 2 is 192.168.255.127, so an address of 192.168.255.10 would work as an example.
- Connect Port LAN 2 to the network or directly to the computer with the discovery tool.

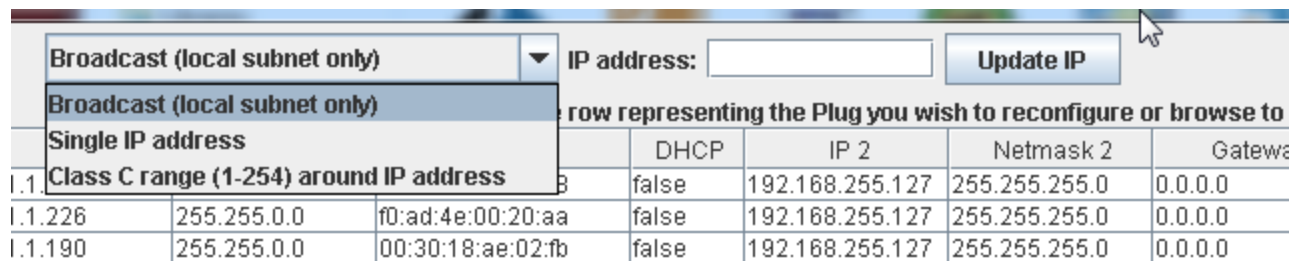


- The computer should NOT have any additional addresses in the same subnet as is being used, for example a wireless IP. If it does have a second address in the same subnet, disable that NIC during configuration.
- The appliance should also NOT have a second IP in the same subnet, even if the other port is not connected. This is the factory default condition.
- Launch the discovery tool.
- Configure the appliance (below)

### Using the Discovery Tool Utility to Configure the Appliance

The tool will Discover Appliances found on the network using three choices for discovery method:

- [DEFAULT] Broadcast only works when the appliance and the computer running discoverytool.jar are both in the same subnet. The IP address field is ignored in this mode.
- Single IP address will use the IP in the IP address field.
- Class C range will scan a whole class C. To configure a device, found by this method, you must switch to the Single IP method once you find the IP of interest.



row representing the Plug you wish to reconfigure or browse to				
	DHCP	IP 2	Netmask 2	Gateway
1.1.1.1	false	192.168.255.127	255.255.255.0	0.0.0.0
1.1.226	false	192.168.255.127	255.255.255.0	0.0.0.0
1.1.190	false	192.168.255.127	255.255.255.0	0.0.0.0

Selecting one of the lines in the Appliance Discovery Tool with a left mouse click and then selecting the Adjust IP Parameters button will open the Update IntraVUE Appliance IP Settings display. The correct “Use IP 1” or “Use IP 2” must be set at the bottom of the discovery tool.

**Update Intravue Plug IP Settings**

**MAC 1**  ☒ **Use DHCP**

**IP 1**

**Netmask 1**

**MAC 2**  ☐ **Use DHCP**

**IP 2**

**Netmask 2**

**Default Gateway**

**DNS Server**

**Password**

**Cancel** **Submit**

In this dialog the IP addresses (uplink and downlink), Subnet Mask, and DHCP settings can be adjusted for both ports.

In addition, a global Default gateway and DNS server IP address can also be configured if required. In many applications where there are isolated networks these would be left all zeros.

To save the settings enter the password [default: 'intravue' (case sensitive)] and select Submit.

To continue with configuration, you must first determine whether you are configuring your Appliance as an IntraVUE Server or as an IntraVUE Agent. What's the difference?

## Updating the IntraVUE Appliance Image

To update your IntraVUE Appliance to the latest version follow these steps:



Before updating your appliance make save a backup of the current database. See [Generate Support Archive](#)

1. Download the update package from the [IntraVUE™ downloads](#)
2. Go to "Download for Appliance/Agent/Plug"

3. Select the latest version and extract all files
4. Go to the ..\applianceonly\_2.4.1a9 folder and locate your appliance using the agentconfig\_all.jar (Agent Discovery Tool). See Instructions above.
5. Open plugupd\_all.jar and point the target IP to be that of the IntraVUE appliance.
6. Select 'Appliance' and 'Use tgz File' options and leave 'Preserve user data' checked.
7. Click 'Start Upload'
8. Wait for 'Finished' message
9. Click 'Intravue Browser'

## Creating Plant Documentation

## Export / Import

The Export / Import features are accessed from the Configure > Database Menu. This brings up a dialog which enables you to export device properties from IntraVUE™ or import device data to IntraVUE™ from other sources.

**DATABASE CONFIGURATION**

Auto-backupClearRestoreBackupExport/ImportArchive

ExportImport

EXPORT INTRAVUE DATA TO A CSV FILE

DEVICE INFORMATION

☒

DEVICE CONFIGURATION

☒

INCLUDE N/A NODES

☒

WEBLINKS

☒

PLANT LAYOUT COORDINATES

☐

FILENAME

HVAC\_Bulk\_Export

Export Data

### Export

If you select the **Export** button, a standard Windows file download dialog will ask if you want to save the file or open it. If Microsoft Excel or similar spreadsheet program is installed, you may open the file directly into that. Export files are saved comma separated value (CSV) format.



By default this IntraVUE™ will export all of the checked boxes except the plant layout coordinates.

To export just specific device properties simply select from the check boxes below what you want to export:

**Device Information:** This will export all devices with its respective device info (i.e. image, other name, vendor, model, description). See [Device Side View](#)

**Device Configuration:** This will export all devices with its respective general settings (email and critical status), advanced settings, & snmp settings. See also [Device Configure - General](#), [Device Configuration - Advanced Tab](#), [Device Configure - SNMP](#)

**Include N/A Nodes:** This will only export 'n/a' nodes. See [NA Nodes](#)

**Weblinks:** This will export all devices with its respective weblinks. See [Device Configure - Links](#)

**Plant Layout Coordinates:** This will export all devices with its respective X-axis and Y-axis coordinates used in the plant layout. See [Creating Plant Documentation](#)

## Import

If you select the **Import** button, the file listed in the filename field will start to be imported. Import files have to be in plain text, comma separated value (CSV) format.



IMPORT AN INTRAVUE .CSV FILE INTO INTRAVUE.

C:\intravue.csv Browse...

ANALYSIS OF IMPORT DATA  
directIpMatches: 0  
isError: 0  
noMatches: 0  
indirectMatches: 0  
ambiguousRecords: 0

Proceed With Import

Data is primarily imported based on the IP address field of the saved file. This makes it possible to import data from files that have been saved from other IntraVUE™'s or from previous databases on the host computer.

If a match by IP address is not possible, IntraVUE™ tries to make a match based on the parent switch and switch port of a field.

Usually only fields for manually inserted devices connected to other manually inserted devices would have problems being imported.

You must select the **Proceed With Import** button to complete the process.



Always import IntraVUE™ exported \*.csv files so that these can be imported back without any problems. This will prevent you from having to modify your regional windows settings to English as some countries (e.g. Germany) use comma as a csv separator instead semi-colon as in the U.S. In any case IntraVUE™ supports both comma and semi-colon separated csv files.

## Import & Export Functions - CSV File

When you look at the exported data in a spreadsheet program you will find many columns. There are 3 basic sections:

- » Reference data
- » Configuration data for each IntraVUE™ 'View'
- » Configuration data from the device's General Tab
- » When saving the file, use CSV as the type and use quotes as the field marker. Don't use quotes in any view names.

Although the export function outputs many columns, you may delete columns you are not interested in EXCEPT the ipAddress, ref, and parentRef columns. These are used during the import process.

You may not change any values to the left of DeviceName. They are shown in the image below.

	A	B	C	D	E	F	G	H	
1	IP	Active	MAC	Ref	ParentRef	ParentIP	ParentPort	UplinkPort	Device
2	10.2.2.1	1	00 00 0C 07 AC 00	5	1		0	0	stswsh
3	10.2.2.5	1	00 80 63 08 CF 3E	232	5	10.2.2.1	23	1	Hirsch
4	n/a	1		256	232	10.2.2.5	7	0	Auto I
5	10.2.2.251	1	00 20 B7 00 18 9A	236	256	n/a	0	0	no nar
6	10.2.2.252	1	00 20 B7 00 18 9E	238	256	n/a	0	0	no nar
7	10.1.1.88	1	00 01 02 6F A2 70	9	1		0	0	WHITE
8	192.168.100.2	1	00 0C 29 3C 97 2A	67	9	10.1.1.88	0	0	vm-ub

- » IP - IP Address or n/a if the line represents an auto inserted node.
- » Active - 1 if the device is currently connected.
- » MAC - MAC Address.
- » Ref - internal database reference number.
- » ParentRef - internal database reference of the device's parent.
- » ParentIP - The IP Address of the device's parent. This will be a switch, router, or the top parent of the IntraVUE™ network.
- » ParentPort - The port number from the parent to the device.



- » UlinkPort - If the parent is a switch, the uplink is the port leading back to the top parent, otherwise it is 0.

It is particularly useful to SORT the exported data by the ParentIP column and then by the ParentPort column. This will give you a list of all your devices arranged by the switch they are connected to, in port number sequence. This is very useful if you want to compare what IntraVUE™ says to what your documentation says.

The next section contains contains columns for names, weblinks, and images. There is one sub-section for each of the 6 views of IntraVUE™. Note there is no column for IP View Name because you can not change that.

I	J	K	L	
DeviceViewName	DeviceViewWeblink1Title	DeviceViewWeblink1URL	DeviceViewWeblink2Title	DeviceViewWeblink2URL
stswshc1.st3483				
Hirschmann RS2	Home Page	<a href="http://hirschmann.com">http://hirschmann.com</a>	manual	/manual
Auto Inserted Node				
no name				
no name				

- » xxxViewName - The name to appear for this view.
- » xxxViewWeblink1Title - name to appear to user in the browser.
- » xxxViewWeblink1URL - url that will be called when the user clicks on the link.
- » xxxViewWeblink2Title
- » xxxViewWeblink2URL
- » xxxViewIconImage - icon image to display for this view
- » xxxViewThumbnailImage - thumbnail image to display for this view

The last section contains items from the Device Configuration General Tab.

AX	AY	AZ	BA	BB	BC	BD	BE
Category	AutoConnect	AutoBootp	IsWireless	SendAlarms	AlarmEmailAddress	SendToDefaultUser	Verifie
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
13	0	0	0	0		0	
13	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	1	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	
12	0	0	0	0		0	

- » Category
- » Auto Connect
- » AutoBootp
- » IsWireless - this corresponds to the WAP checkbox.
- » Send Alarms - to 'this' device's specific receipient.
- » AlarmEmailAddress - email for 'this' device's specific receipient.
- » SendToDefaultUser- to email alarm receipient in the System Configure Email tab.
- » Verified - Admin Verified checkbox.
- » Properties - An encapsulation of several items on the Device's General Tab. This column is not meant to be edited. It is meant to be copied from one device configured the way you want to another device without modification. This includes columns such as 'disable all snmp', 'ignore bridge mib', 'use snmp for mac', and snmp community.
- » PKI.critical - This column is only available when you have enabled critical status for the KPI System on at least one device. See [Device Configure - General](#)

See [CSV Column Values](#) for a list of available values for selected columns

## Importing Device Information other sources

See tech note [Importing Device Names From Third Party Sources](#)

## CSV Column Values

Column Name	Device Configuration Equivalent Value
SNMP.supress	1 - Disable all SNMP requests, 8 - Ignore SNMP Device Name, 4 - Ignore SNMP Location, 2 - Ignore SNMP Bridge Mib data. You can add up all or multiple values and enter that value (e.g. 12 = 8 + 4).
MAC.override	SNMP - "Use SNMP - provided MAC"
PKI.critical	<p>Critical Values for this column in the .csv export are:</p> <ul style="list-style-type: none"><li>0: Unknown</li><li>1: Ignore</li><li>2: Critical Intermittent</li><li>3: Always On</li></ul>

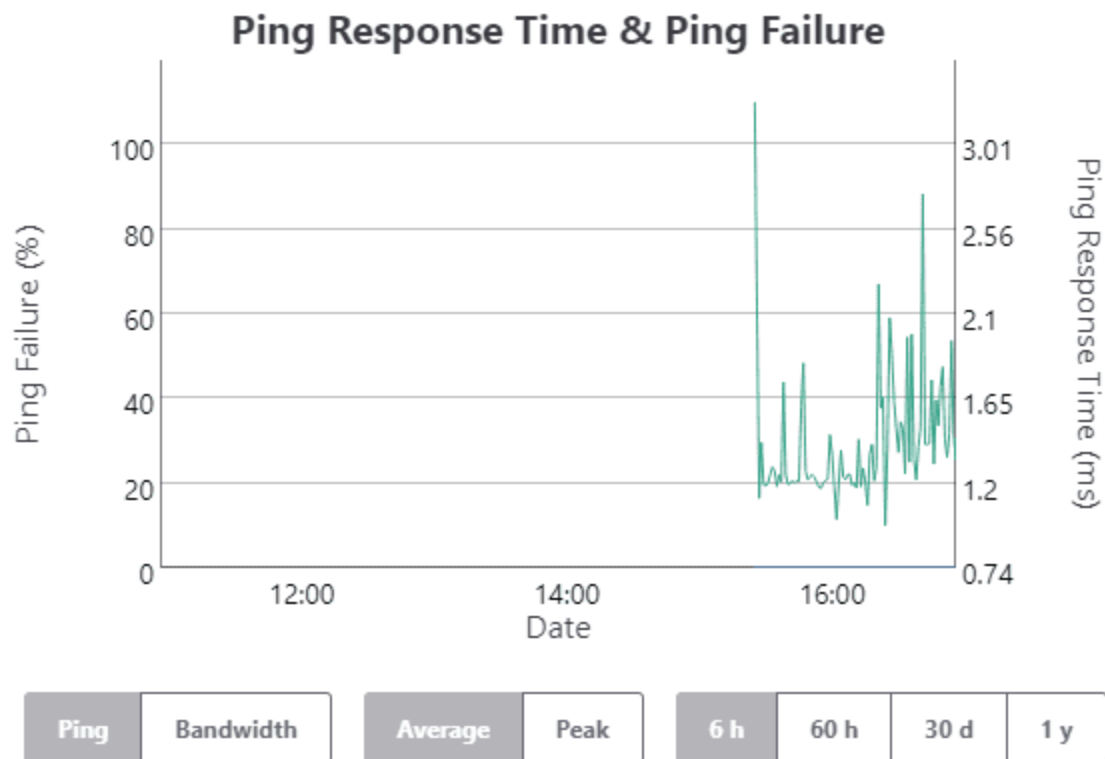
## IntraVUE Diagnostics

## Threshold Graphs

Threshold graphs are broken into two kinds:

**Single Device Graph** - This graph is generated for a single device containing data for pings, or bandwidth, or both

### Graph



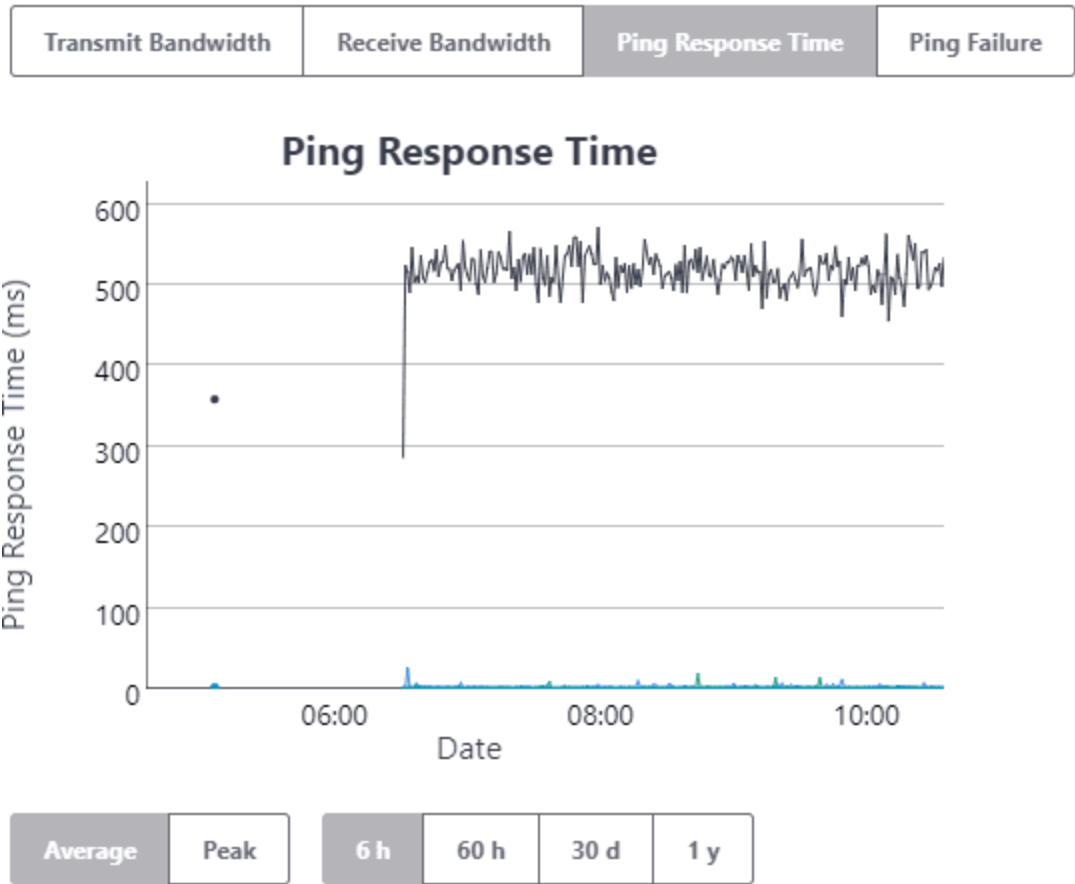
— Ping Failure  
— Ping Response Time

### Threshold Settings

Ping Response Time Threshold (msec): 30

Ping Failure Threshold (%): 20

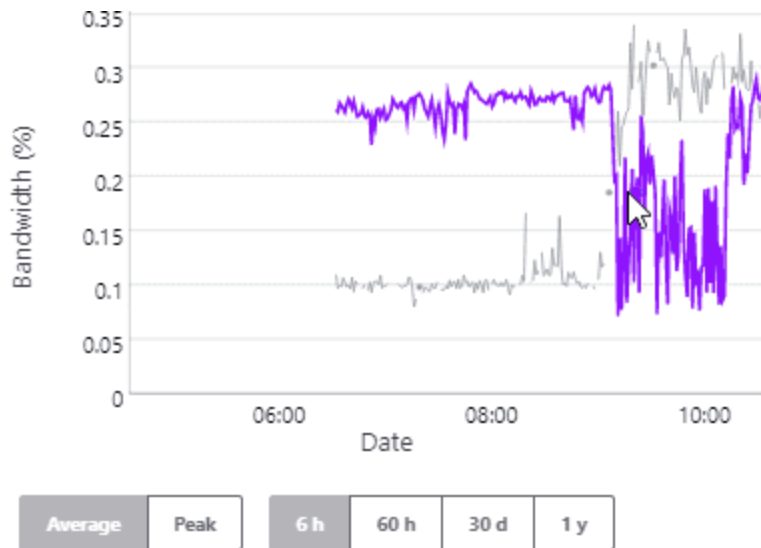
**Multi-Device Graph** - This graphs is generated for multiple devices containing data for pings, or bandwidth, or both. This graph is commonly seeing for a switch (see [Switch Side View](#)) and when highlighting multiple devices (see [Multiple Device Side View](#)).



- 10.1.1.137 - Ethernet Direct Managed Switch
- 10.1.1.188 - N-TRON Managed Switch
- 10.1.1.230 - Historian Server
- 10.1.1.252 - Cisco Managed Switch
- 10.1.1.1 - Cisco Managed Switch

The Multi-Device Threshold Graph is designed to give the user a view of one threshold type for many devices at the same time.

**Hover Over:** When the mouse is positioned on the line, IntraVUE™ will indicate the IP Address and name of the device, and the time of the value as you hover over on the graph.



Jun 2, 2015 9:21 AM:

10.1.1.72 - OP-JSAH-MACBOOK: 0.185693

10.1.1.94 - JESSE-LAPTOP: 0.185693

10.1.1.46 - Scanner 26: 0.185693

**Zoom In:** You can zoom in on any portion of the graph by dragging the mouse with the left mouse button from left to right (horizontal zoom) or from top to bottom (vertical zoom).

**Zoom Out:** When you are ready to zoom out, simply double click on the graph

**Freeze Graph:** You can freeze the graph by clicking on a line once. To un-freeze click again on the graph.

## Graphing Options

The graph is 'live' and updated with new data every one minute.

There are four threshold conditions monitored and displayed by IntraVUE™.

- » Transmit Bandwidth (Xmit) - the percent of available bandwidth used for transmitting.
- » Receive Bandwidth (Recv) - the percent of available bandwidth used for receiving.
- » Ping Response Time - the response time to a ping request from the IntraVUE™ host to the device.
- » Ping Failure - the percentage of failed pings in a one-minute period.



**Bandwidth data** is collected once per minute from every device having SNMP and additionally from every switch port that has a 'child' device under it. If a devices does not support SNMP but is connected directly to a managed switch, the bandwidth data is collected from the parent switch.

The device that provides the SNMP information is identified by (Datasource) on the Connection From/To lines.

Transmitted data is the data from the parent or 'from' device regardless of the data source.

**Ping data** is collected many times per minute, typically 5 to 10 times. This successful pings in a one minute period have their response times averaged and that one minute average is used as one data point for Thresholding. If a ping is unsuccessful and the next ping is successful, it is counted as one ping failure. Over the course of the one minute period the number of failures divided by the number of pings in the one minute period becomes the Ping Failure rate for that one minute period. (If two successive pings fail, it is recorded as a device disconnect.)

### Average or Peak Values

As data becomes older it is averaged into larger time period samples. At the time of averaging the peak value during the period is also stored. When viewing the data you can use the two buttons interchangeably to choose the average for a period or the peak for a period.

### Data Resolution

The data is stored internally in a way that progressively creates historical data from more recent data. Over time data kept in seconds format is averaged to become minute format, minute data becomes 10 minute data, hour data becomes day data, and so on.

Below the Update button is the Time Scale drop down list. Selecting this control will display the following time intervals and data resolutions:

#### Choice for Data Resolution

Selection	Data Resolution
6 hours	2 minute points combined

60 hours	2 10 minute points combined
30 days	2 2 hour points combined
1 year	2 day points combined

### Graph Vertical Scale

At the top of each graph is the graph full scale value. This value will change as the data being presented is updated. It is designed so that the greatest actual values are near the graph top.

As you cycle between the threshold dialogs of several devices the graph max values will change to provide you the best data for interpretation

### Transmit Bandwidth

In the example above the bandwidth graph's scale is close to 1.000 percent bandwidth and the bandwidth thresholds is set at 30.00 percent. If there had been a spike to 22 percent in the Xmit bandwidth in the 6 hour period shown, the scale would have been set to about 25.0 percent so you could see all the data without exceeding the graph max.

### Ping Graphs

For Ping statistics the Ping Failure percent and the ping response times are both shown in the same graph. The graph max for Ping Failures is always 100%, shown on the left. The graph max of the Ping Response data varies similar to Bandwidth in that the scale changes so the maximum amount of significant data is visible.

### Setting Threshold Values for this device

The Edit button is selected by the Administrator after any change to the threshold settings and will update the database for the new settings. Be careful the graph does not update just as you select update.

## Multiple Device Side View

When you headlight two or more devices you get this side view where you can restrict ping and bandwidth performance just to the selected nodes.



**Delete These Devices** - When clicking this button you can delete all of the highlighted devices after you accept the confirm delete message on the button.

The Ping and Bandwidth graphs are only computer for the IP addresses highlighted and their values are shown depending where you hover over your mouse of the graph (see [Threshold Graphs](#)).

If you believe a device should not be highlighted simply turn off the green toggle button for that device and will be removed from the graph.

If you click on the down arrow on each device you can see the device info. See [Side View in Edit Mode](#)

## Generate Support Archive

When you select this item from the Navigation bar > Configure > Database > Archive you may Download or upload a Support Archive file.

TA Database Email General Advanced

DATABASE CONFIGURATION

Auto-backup

Clear

Restore

Backup

Export/Import

Archive

Create Archive

Send Archive

Upload Archive

To create a system archive file, click the button below. Note: It may take as long as 3 minutes to generate the archive file. Please be patient....

Create and Download Archive

### Create Archive

When you click the **Create and Download Archive** button, a backup is then added to a zip folder having the file ending of 'zzz'. This is really a 'zip' file, but the extension name is changed so it can pass more easily through virus and email checking programs. To this zip file a number of other files are added. Some are configuration files and others are log files. These files provide technical support and others a more complete picture of IntraVUE.

When all the files have been generated and stored in the zip file, the dialog will change to "Archive file created and downloaded" and a windows dialog will allow you to open or save the file. Select 'Save' and the next dialog will allow you to specify the folder of your choice. You may even rename the file if you like.

### Send Archive

This feature allows you to upload a previously created IntraVUE archive file to Panduit's Analytical Reports engine which will create an analysis report that identifies potential issues in your network.

Simply click on the link below that will open a new tab where you will have to login or sign up and follow the prompts to generate an analytics report. See

### **Upload Archive**

The Upload Archive function is used to upload a previously downloaded archive that may contain modified files, such as trunkingdefs.txt or a backup saved on a different computer. If you select this button, you will be able to navigate to the archive file to upload on the IntraVUE system and then load the database (C:\intravue\dbbackup\\*.dmp) file under the Configure > Database tab.

## Event Log Descriptions

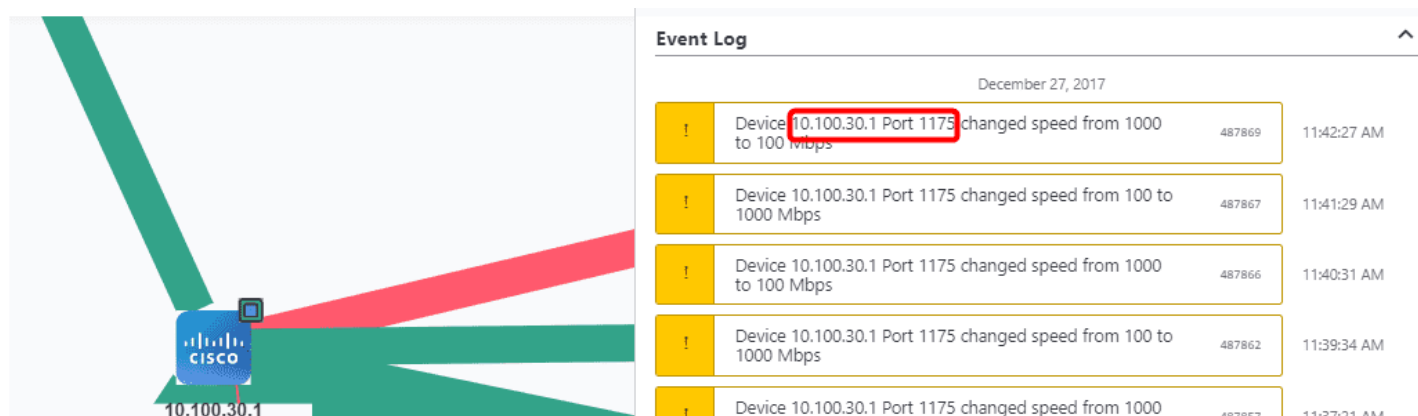
### Device x.x.x.x disconnected

This event is generated when a device (by IP address) reached a 100% ping failure threshold and IntraVUE™ cannot continue monitoring such device.

### Device x.x.x.x reconnected

This event is generated when a device (by IP address) recovered from a 100% ping failure threshold and thus IntraVUE™ can continue monitoring such device.

### "Device x.x.x.x. Port yyyy Changed Speed From X to Y Mbps"



Devices with Link Speed Changes causes these types of events due to many reasons including:

- » Duplex mismatch - Set both to the same duplex setting or Auto (e.g. 1 GB links)
- » Port speed mismatch - Set both to the same speed or Auto (e.g. 1 GB links)
- » Check for bad connectors, poor cabling, or cabling longer than specification
- » Misconfiguration on Firewall (ICMP packets are being dropped)
- » Device or Switch recently powered ON or OFF (One time)
- » Device or Switch resetting (confirm drops around same times with bandwidth and ping graphs)
- » Bad device - The device connected to that port would show disconnects on its event log and

lots of ping failures and disconnects on the connection graphs going to that bad device

- » Bad switch. This would also create duplicate IP messages (i.e. "Changed Mac from" events).

### **"LLDP: Device x.x.x.x moved y.y.y.y"**

Devices that make use of the LLDP protocol fire this event whenever there is a move action. See

[Supported Protocols](#)



# IntraVUE Diagnostics

IntraVUE provides a method to record and capture the issues that occur in the Ethernet networks being used for automation applications. Automation networks are susceptible to subtle disturbances due to the real time nature of the applications, as well as the timing requirements of the connected equipment. Environmentally created problems, as well as “cause and effect” actions can create intermittent disturbances that will be hard to detect by conventional networking tools.

Although IntraVUE can provide an accurate assessment of the connected devices and their inter-connections, it is the ability to sense problems on the network that provides the greatest value. IntraVUE has helped quickly identify many common problems in these automation networks. The following covers the variety of issues identified by IntraVUE and how they are represented. These include:

1. Device failure
2. Duplicate IP Address
3. Broadcast or Multicast Storm
4. Intermittent Connection problems
5. Devices accidentally moved
6. Foreign computers momentarily linking to the network
7. Large File transfers between devices
8. Bad RSTP, Ring Switches, or accidental cable loops
9. Resetting Switch
10. Overloaded or misbehaving devices

## Device Failure

Device failures are common in any system. The key issue in an automation system is getting the failed device back up and running. This is especially important if the device has shut down a production line. The typical first responders are technicians who understand the devices but who may not have a great deal of network experience. It is thus important to provide the details so that the device can be reset or replaced .

IntraVUE provides a live animated graphic that can show a disconnected device by a red line. Hovering over the line will provide details as to the port on the switch the device is connected. Figure 1. A first check would be to see if the connection to the switch is still made. Many times a disconnected device may be as simple as a connector dislodged as someone works on the switch.

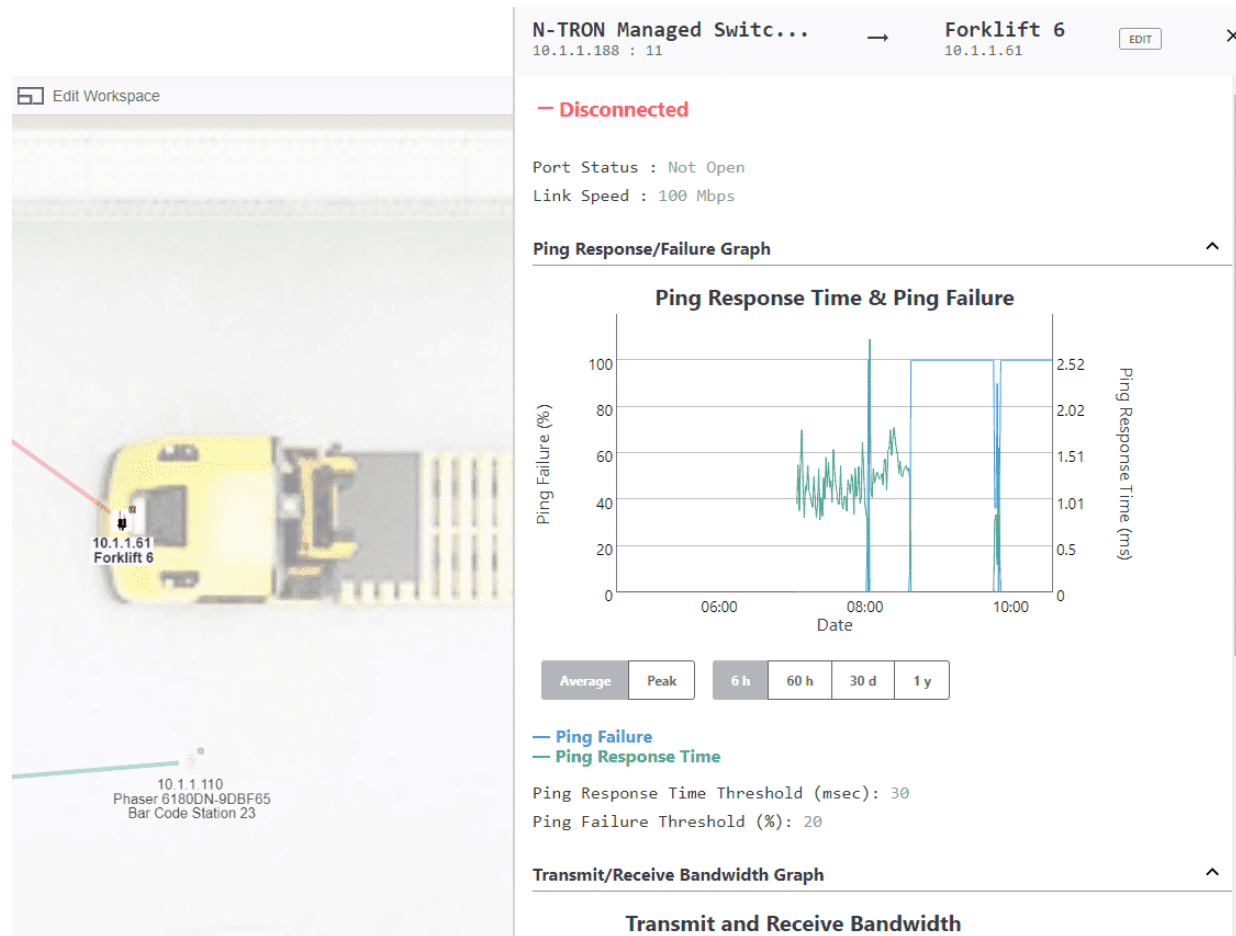


Figure 1. IntraVUE Visualization.

Additional details can be obtained on the time of the disconnection and if there have been several intermittent disconnections prior to the failure by opening up the event log. This information can be easily achieved by right clicking on the device and bringing up the event log for the device. The event log will contain a time based history of the device. The history can cover many months and thus if there are repeated issues they can be reviewed (Figure 2).

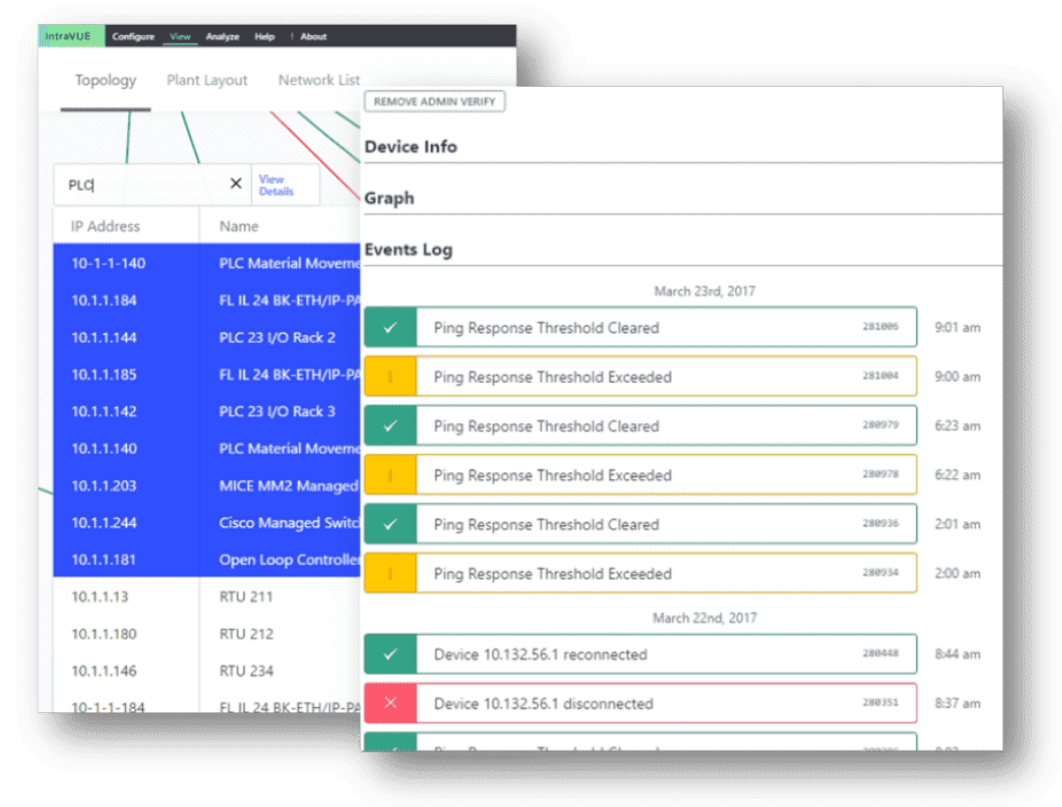


Fig 2. IntraVUE event log.

To obtain additional details for the affected device such as a maintenance log, user manual or other repair procedures one can click on the properties of the device (Figure 3).

The Properties window can provide the IP address and MAC address of the device as well as Vendor and Model. Since IntraVUE is a Web Server this data is available to any computer that can browse to the IntraVUE system. It provides both technicians and Control engineers a common tool to quickly resolve basic problems.

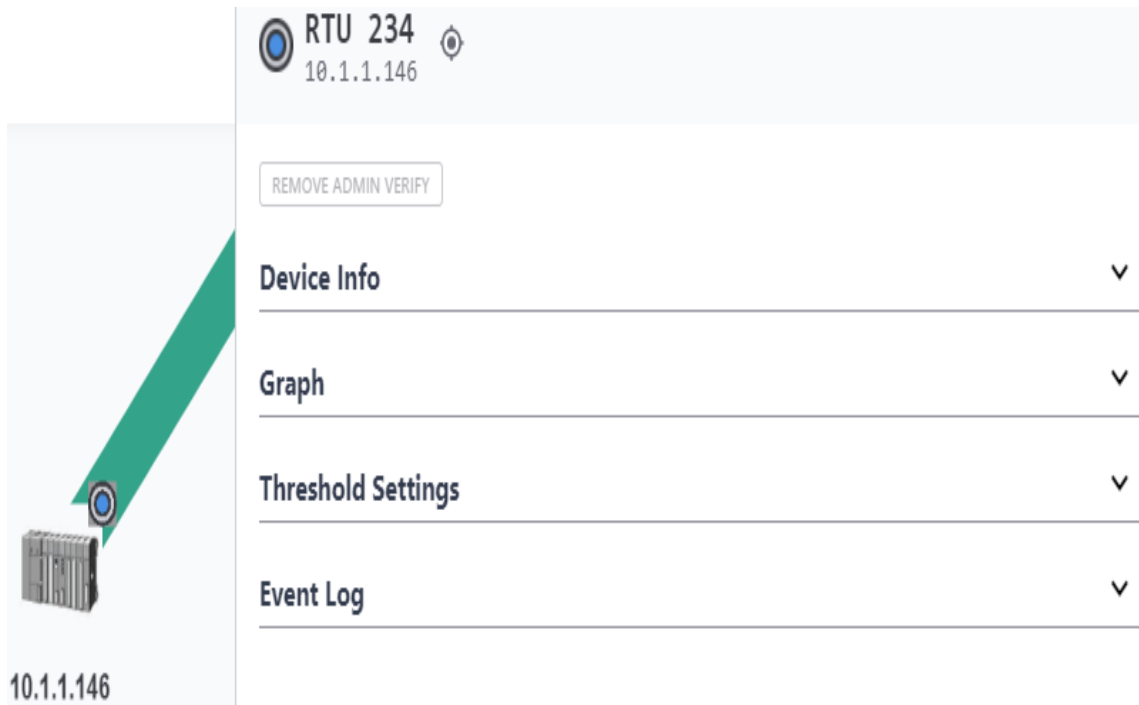


Figure 3. Device properties.

### Duplicate IP Address

Most devices in an automation network will have static addresses. Since for the most part assigning an IP address to a device is a manual process, the chances of a device getting an address that is in conflict rises as the number of devices increase (Figure 4a). Duplicate addresses can create a great number of issues and should be avoided. It is thus important to quickly identify if a duplicate address has been added on your network.

IntraVUE can help quickly identify a duplicate address by tracking the IP, MAC and location of all devices on the network.

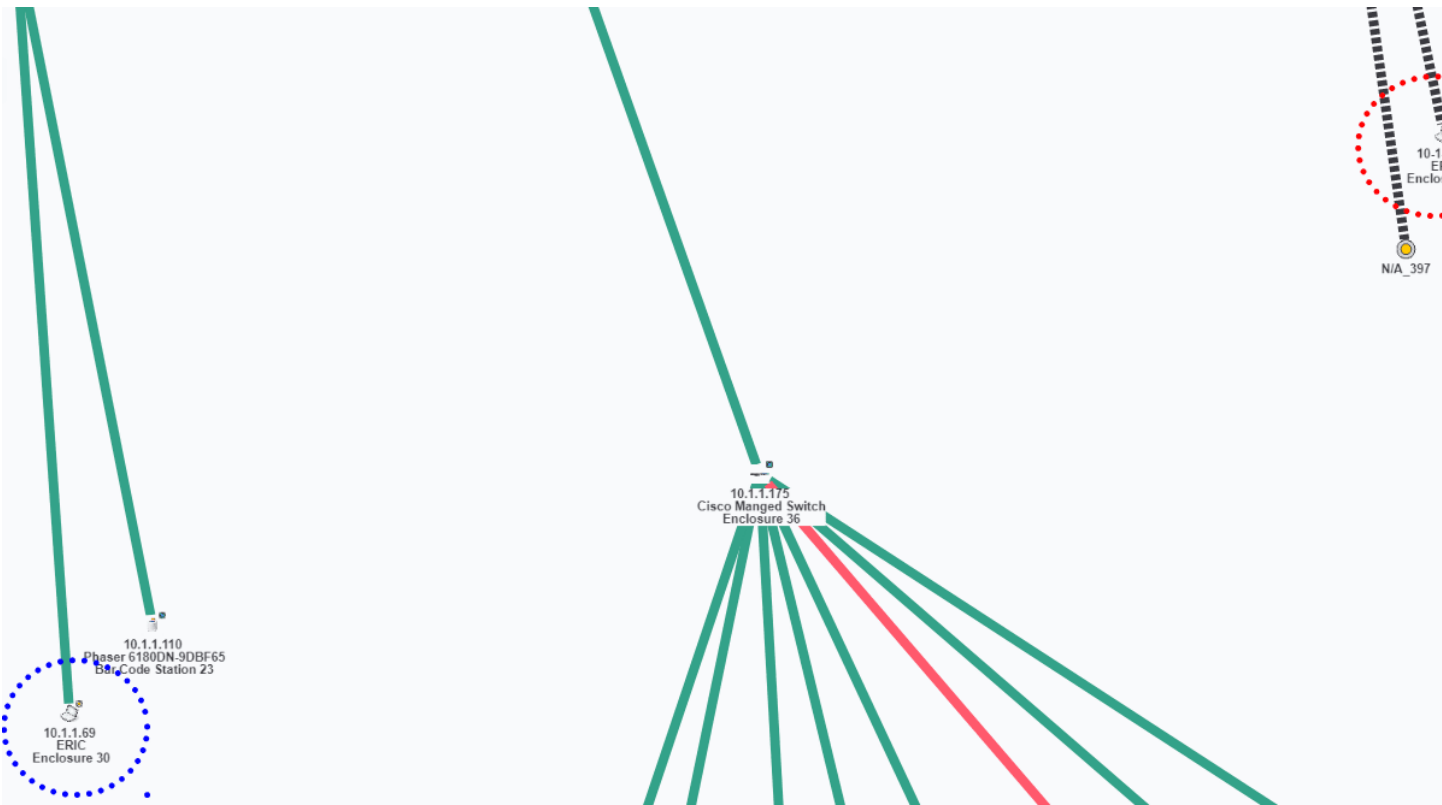


Figure 4a. IntraVUE showing a duplicate address in Map View.

IntraVUE				
Configure	View	Analyze	Help	About
Warning - data is not current. Scanner is in OFFLINE mode. Demonstration Version - Not for Commercial Use				
Topology	Plant Layout	BETA	Filters	Event Log
changed				
ID	Date/Time	IP Address	Description	
4817	Jun 2, 2015 11:21:29 AM	10.1.1.72	Device 10.1.1.72 changed mac from e0:06:e6:c7:30:94 to 28:5a:eb:40:d1:df	

Figure 4b. Duplicate IP address confirmed in event log.

IntraVUE will mark an IP address that appears in two locations with a red box as seen above. By selecting the event log you will see the two MAC addresses listed for an IP Address. This provides details of not only a duplicate address but the location of both devices and the time the conflict was first reported.

This information is also presented in the Diagnostic Report (Figure 5). The report will use the data collected and by determining that an IP address is switching between two MAC address as well as

changing locations in the network. The Diagnostic Report will create a red text to easily identify a duplicate address. See below:

### 3.3.3. Addressing Issues

**Changed MAC addresses (potential duplicate IPs):** *These devices had changes in their MAC address in the last 30 days which might indicate a duplicate IP address. If this device has also been reported in the 'Device Moves' section, it is VERY likely to be a duplicate ip address.*

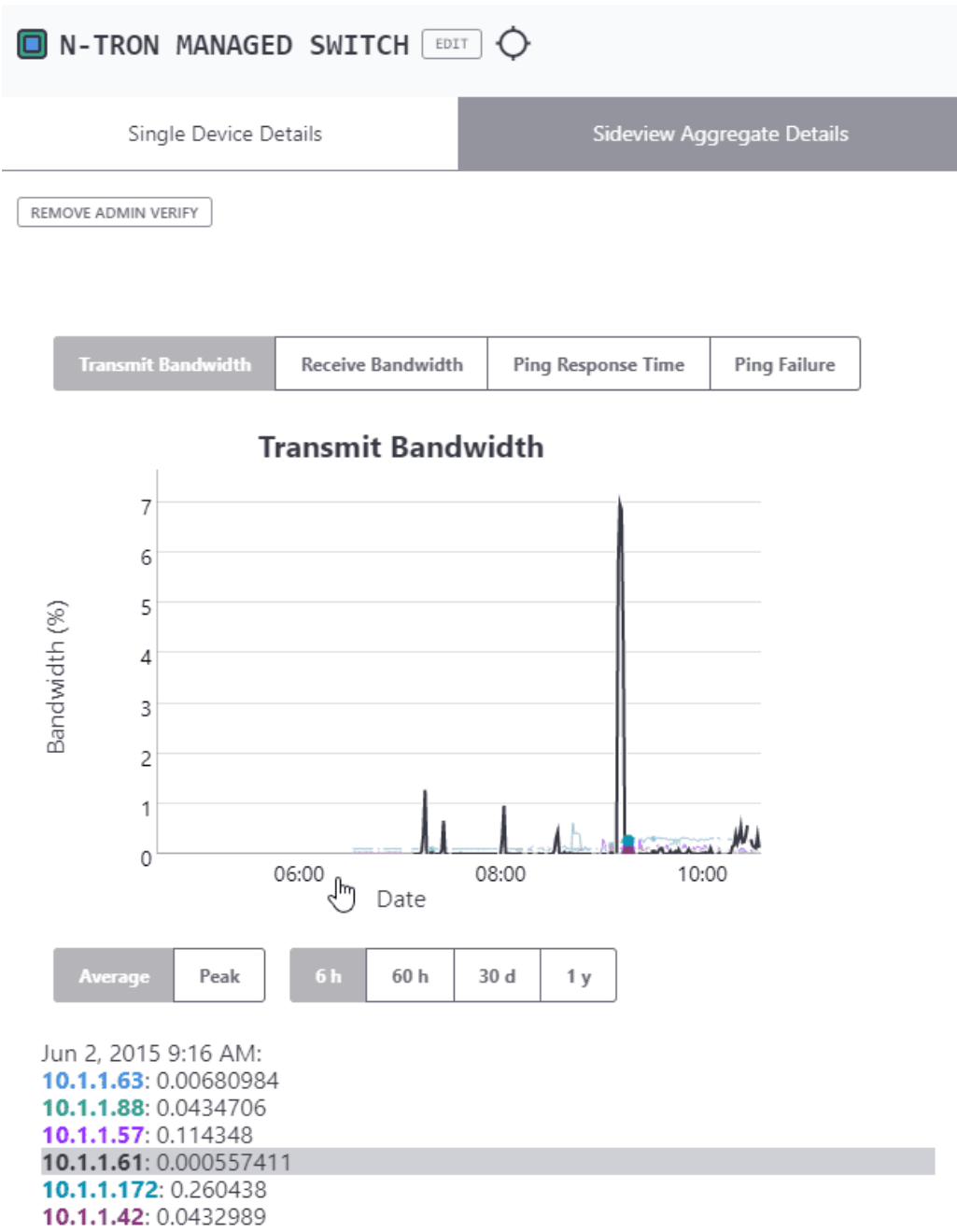
**WARNING: IP 10.1.1.49 has move and mac change events and is probably a duplicate IP.**

10.1.1.49	
2011-09-13 09:47:32.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd
2011-09-13 09:50:51.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:20:cd to f0:ad:4e:00:21:23
2011-09-13 16:50:52.0	Device 10.1.1.49 changed mac from f0:ad:4e:00:21:23 to f0:ad:4e:00:20:cd

Figure 5. IntraVUE Diagnostic Report confirming a duplicate IP address.

### Broadcast or Multicast Storm

At some times a device may generate a burst of broadcast or multicast traffic which will be received by many devices. The transmitted data may only last a short period of time and thus can be hard to find if not continually scanning for the occurrence. IntraVUE records and stores all of the transmitted and received levels on a minute basis and this recorded data can be used to determine not only the sources but also what devices may have received the bust. Using the Threshold Graphing feature one can choose to view all devices transmitting over time. In figure 6 you can see a single device generating a burst of traffic that exceeds 50% of the available bandwidth.



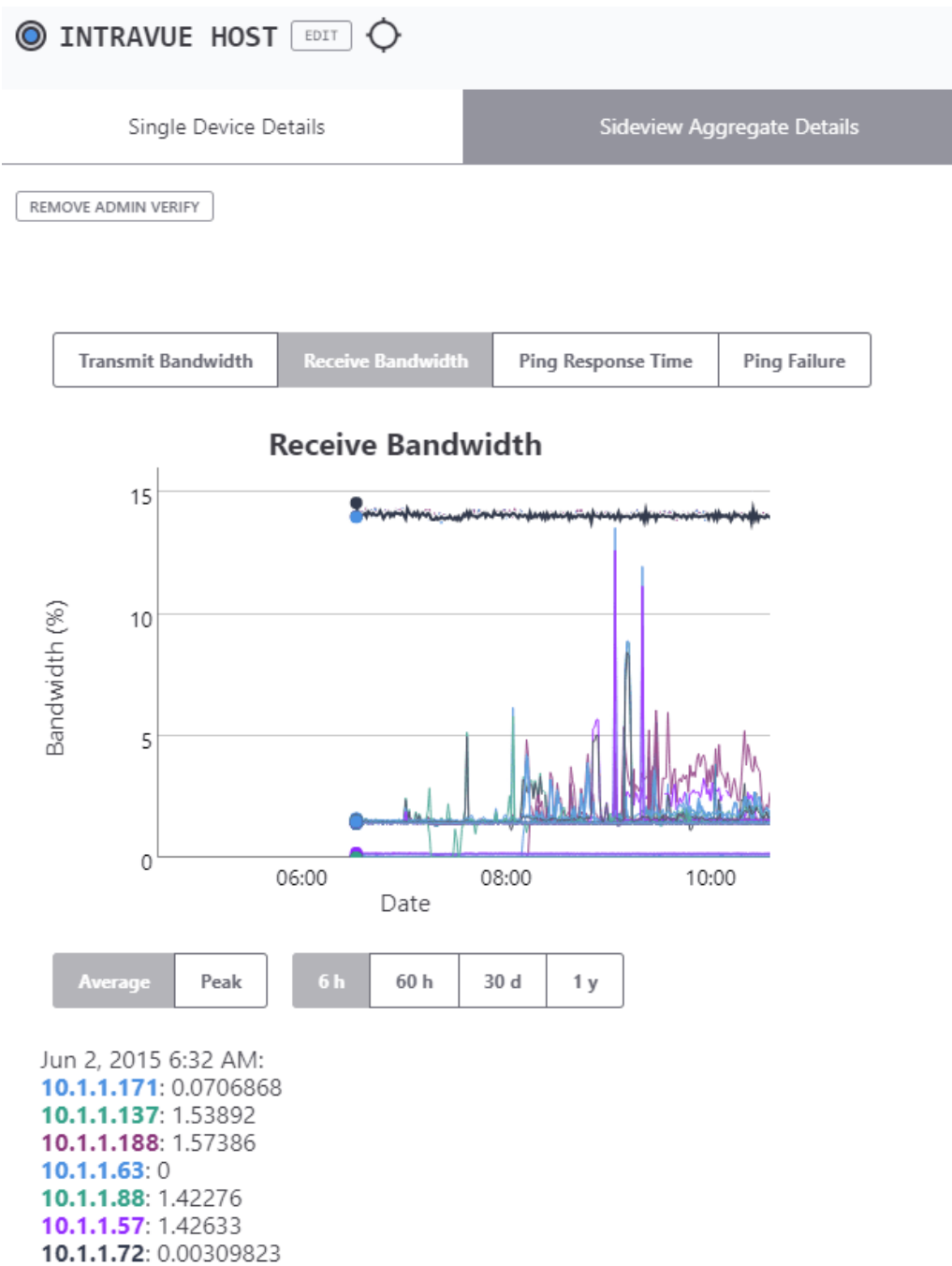


Figure 7. Received data affecting many devices on the network.

If one were to use the Diagnostic Reporting system (Figure 8) the data would have been presented in a table in which the IP addresses of all the affected equipment would be identified.



**Potential broadcast storms in last month:** *Reporting times when at least one device has more than 50.0% transmit bandwidth and at least 3 other devices have greater than 50.0% receive bandwidth (Switches excluded).*

From 2010-01-28 05:30 To 2010-01-28 05:30 0 minutes		Transmit	Receive
10.243.38.120		0.1	52.5
10.243.38.172		0.0	52.8
10.243.38.121		0.0	52.5
10.243.38.190		0.1	61.7
10.243.38.200		0.0	61.6
10.243.38.197		0.0	61.6
10.243.38.224		53.2	19.6
10.243.38.97		0.0	59.1
10.243.38.195		0.1	61.6
10.243.38.247		0.0	52.2
10.243.38.173		0.0	52.4
10.243.38.242		0.0	52.2
10.243.38.241		0.0	52.2
10.243.38.240	Dry Pet Palletizer 2 PLC	0.0	52.2

Figure 8. Shows sources of broadcast storms.

### Intermittent Connection problems

Based on the environment which may contain vibration, electrical noise, and moisture many industrial devices can experience intermittent connection problems. IntraVUE continuously pings all the devices that have been found on the network between 8 and 12 times a minute. Each minute the results are compiled in a percent % failure rate per minute and stored in IntraVUE. In a good network there should be no ping failures. Ping failure percentages can be trended in a graphed to identify if there are connection problems (Figure 9).

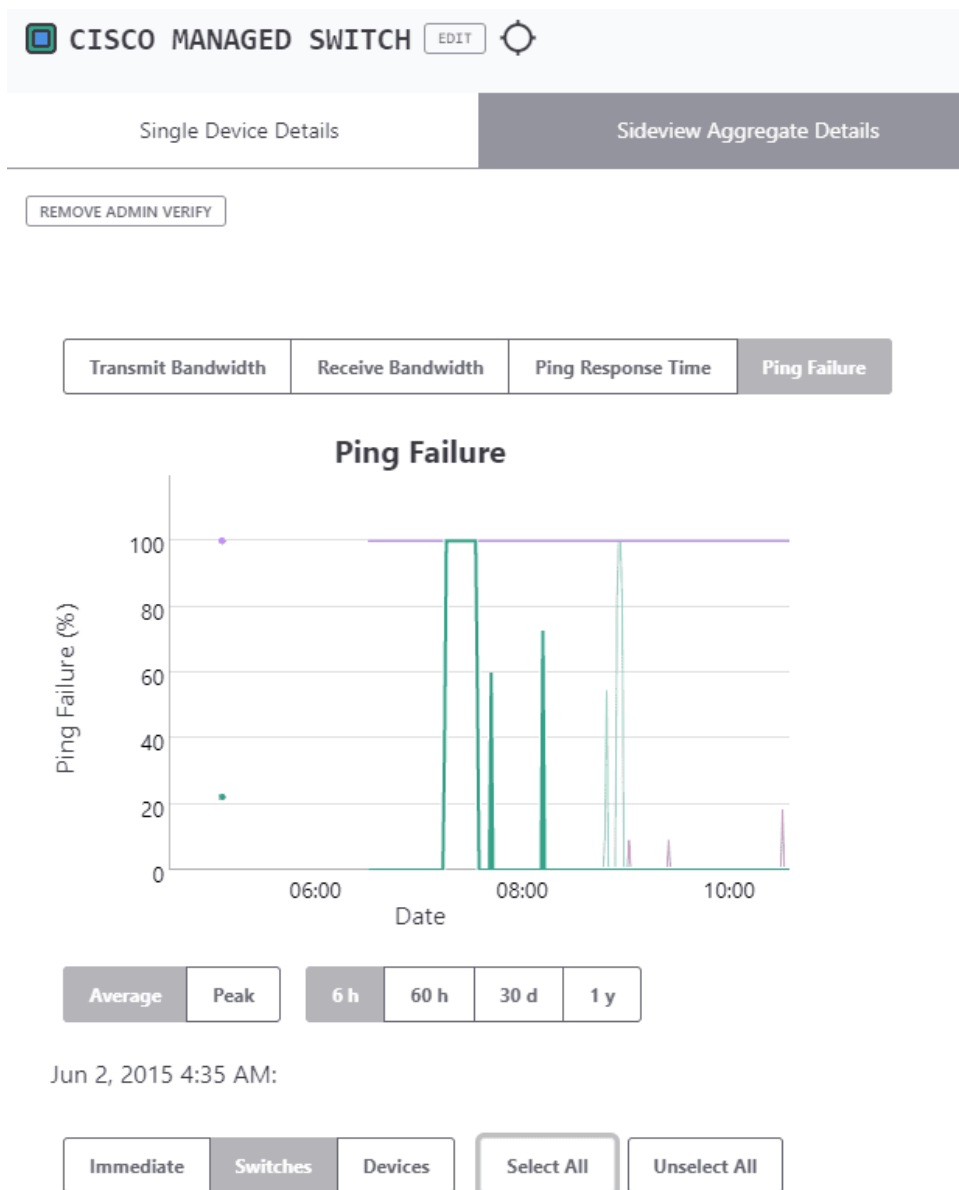


Figure 9. Time based view of Ping Failures

These graphs can help pinpoint the time and frequency of failures that help identify the potential causes. These can be created from environmental issues such as vibration or electrical noise from a large motor or a switch performing auto-negotiation based on a poor link. It can also display if a group of devices are affected at the same time which can point to a specific event or cause.

The diagnostic report (Figure 10) will list the devices with the highest connection problems. The list will contain the failures that have occurred over the last 6 hours, 60 hours and 30 days to determine if the faults are recent.

### 3. VLAN680

**Devices with connections issues:** *Reporting devices that have the highest connection problems (ping failures). You may want to check the connections, wire, and port speed settings to minimize or eliminate these issues*

*In the future, connection issues may be broken into classes such as consistent and intermittent.*

Devices with Ping Failures				
		30 Day	60 Hour	6 Hour
IP Address	Device Name	2 hr counts	10 min counts	1 min counts
10.243.38.173		37	8	3
10.243.38.27	US516234	29	5	
10.243.38.217		24	4	4
10.243.38.11	USDNYFAS516238	18	5	
10.243.38.204		13	2	1
10.243.38.20	USDNYFAS514678	12	4	
10.243.38.208		8		3
10.243.38.207		8		3
10.243.38.222		7	2	2
10.243.38.223		7	2	2
10.243.38.112		7	1	2
10.243.38.103	ConnectUPS Web/SNMP Card	6	1	2
10.243.38.148	USDNYFAS516217	8	1	
10.243.38.180		3	1	2
10.243.38.181		3	1	2
10.243.38.85			2	2

Figure 10. Report showing the most problematic devices.

#### Devices accidentally moved

Many devices in an automation network are fixed to a specific port of a switch. In many cases the port is configured with a speed and duplicity that matches the unique requirements of the device. In other applications the port may be assigned to a specific VLAN. Many of these switches are located in electrical enclosures and additional devices are added frequently. The potential for a connection to be accidentally changed due to device additions or just servicing the switch is becoming more common. In other cases we have seen equipment such as Printers/labelers moved to another line (Figure 11),

which have created other issues when the original line is started and that equipment is expected to be there. Keeping track of equipment can be challenging.

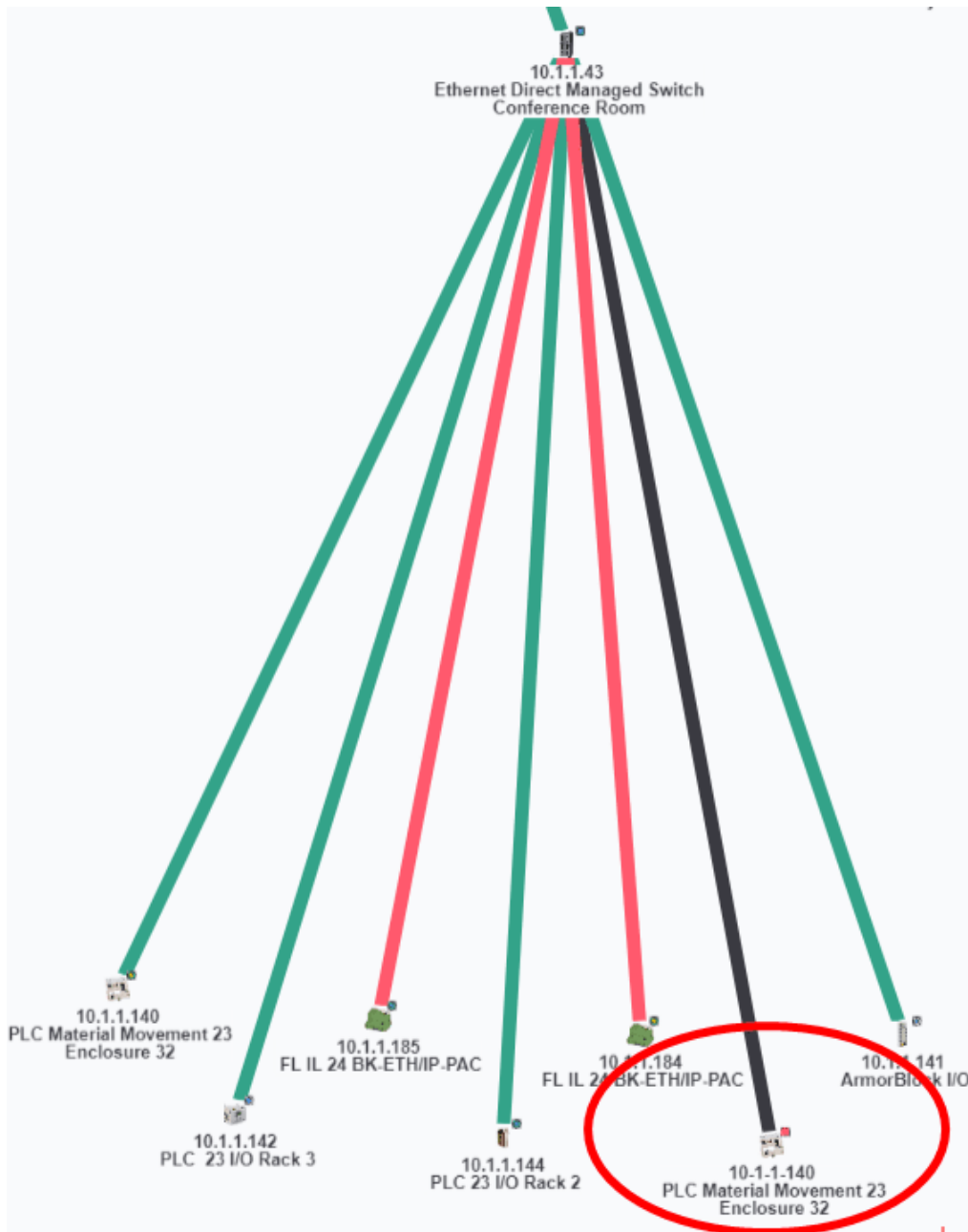


Figure 11. A machine move reflected in IntraVUE.

IntraVUE monitors the moves and provides a graphic indication if a device is moved. The picture on the left shows a Red Box to mark an unauthorized move and hovering over the connection shows the new port.

By selecting the Event Log for the device you can also get the day and time that the move was made. This may help identify details to avoid the move from happening in the future.

Diagnostic Reports (Figure 12) also provide a list and time of device moves. It can provide a very easy way for maintenance technicians to obtain a list of devices that have moved along with key data on the time and the original location.

**Device Moves:** *Reporting devices which moved in the last 30 days which are admin verified and not enabled for automatic moves.*

*Configuration Note: If any of these devices are allowed to move, the IntraVUE administrator should check the Auto Connect checkbox in Device Configuration.*

10.1.1.49	
2011-09-13 09:48:59.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 192.168.200.174:21
2011-09-13 09:51:20.0	Device 10.1.1.49 moved from 192.168.200.174:21 to 10.1.1.136:2
2011-09-13 16:51:36.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 10.1.1.171:49
2011-09-13 16:54:31.0	Device 10.1.1.49 moved from 10.1.1.171:49 to 192.168.200.174:21
10.1.1.106	Drive 234
2011-09-13 08:45:50.0	Device 10.1.1.106 moved from 10.1.1.96 to 10.1.1.244:9
10.1.1.160	oldlinux
2011-09-13 08:41:44.0	Device 10.1.1.160 moved from 10.1.1.252:3 to 10.1.1.252:2

Figure 12. Devices moves reflected in Diagnostic Reports.

### Foreign computers momentarily linking to the network

Security is important for any network. Although many automation systems are behind a firewall and have no access to the outside world, it does not mean they are fully protected. Outside suppliers can easily connect to the network. Even if the switches are locked in protected areas, one can use an Ethernet connection to an idle device to gain network access.

In many cases they may have the right to attach to the network but may inadvertently create a problem such as bandwidth problems when uploading a program or configuring a device. In some cases the foreign computer may only be on the network for a short time (Figure 13). Trying to identify an issue caused with the device now disconnected can be difficult.

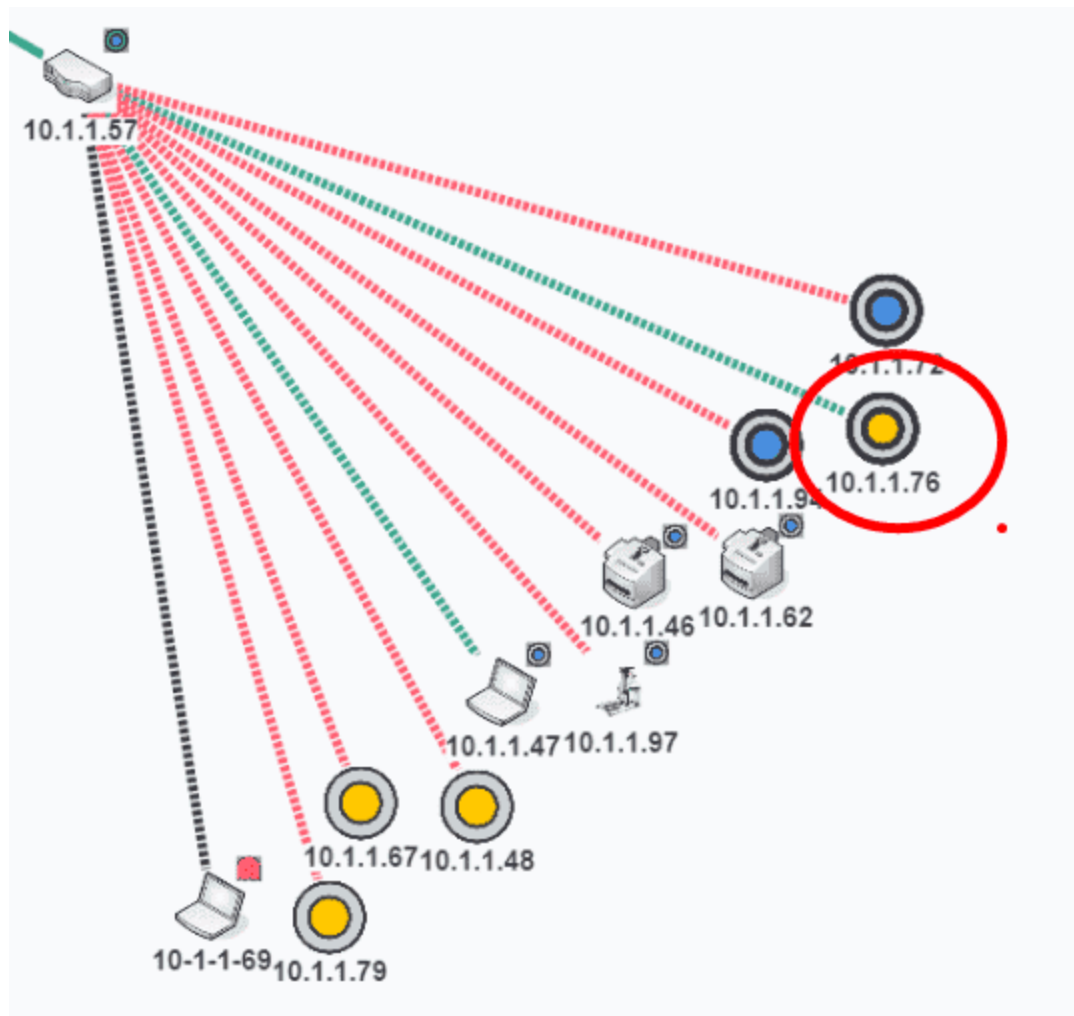


Figure 13. New device detected by IntraVUE.

IntraVUE identifies new devices with a tan colored box which is differentiated from the admin verified blue colored boxes. If the device is still connected to the network the line to the device would be green. A red line will indicate that the device is no longer communicating on the network. Clicking on the Event Log will provide details on the time the initial connection was made and if the device was moved to different locations in the network. If the device created traffic that exceeded the default presets it will also be logged and date stamped.

### Large File transfers between devices

Large transfers between devices could affect network performance by overloading switch traffic. These transfers may occur for a few minutes and disrupt other applications. Disruptions can be seen

as a slowdown in communications or can actually lock up devices. As more devices are connected and use the network for management and configuration as well as Enterprise system gather reporting data the traffic flow can be unpredictable.

IntraVUE can provide specific details on the interaction hours after the event occurred. Many times there is no one immediately available to determine the source of the issue. The recording capability of IntraVUE can provide a time based view of the transmission and receiving of large amounts of data. In the two pictures (Figure 14 & 15) one can see that there was a transfer between two devices that occurred at two separate times in the graph.

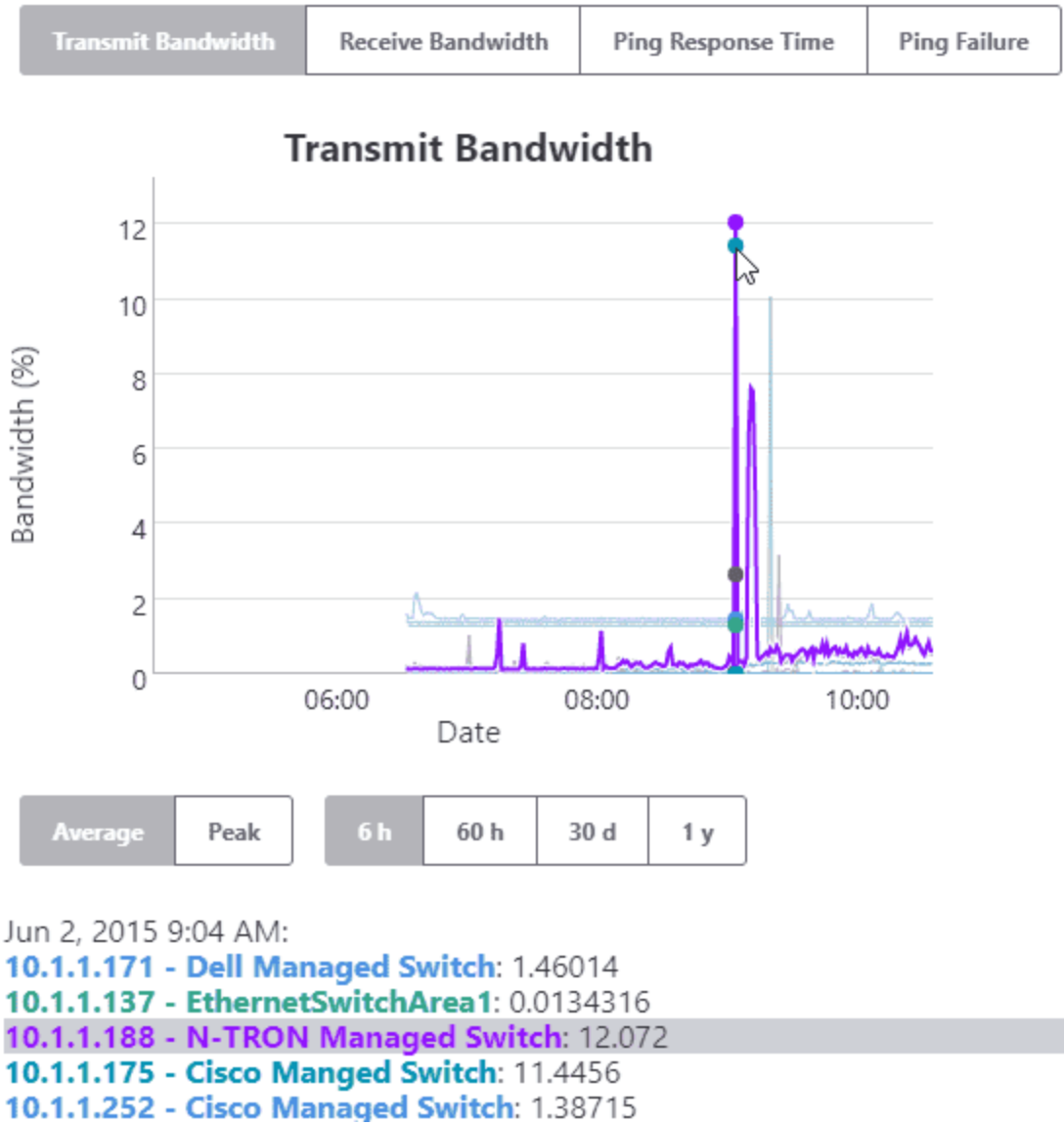
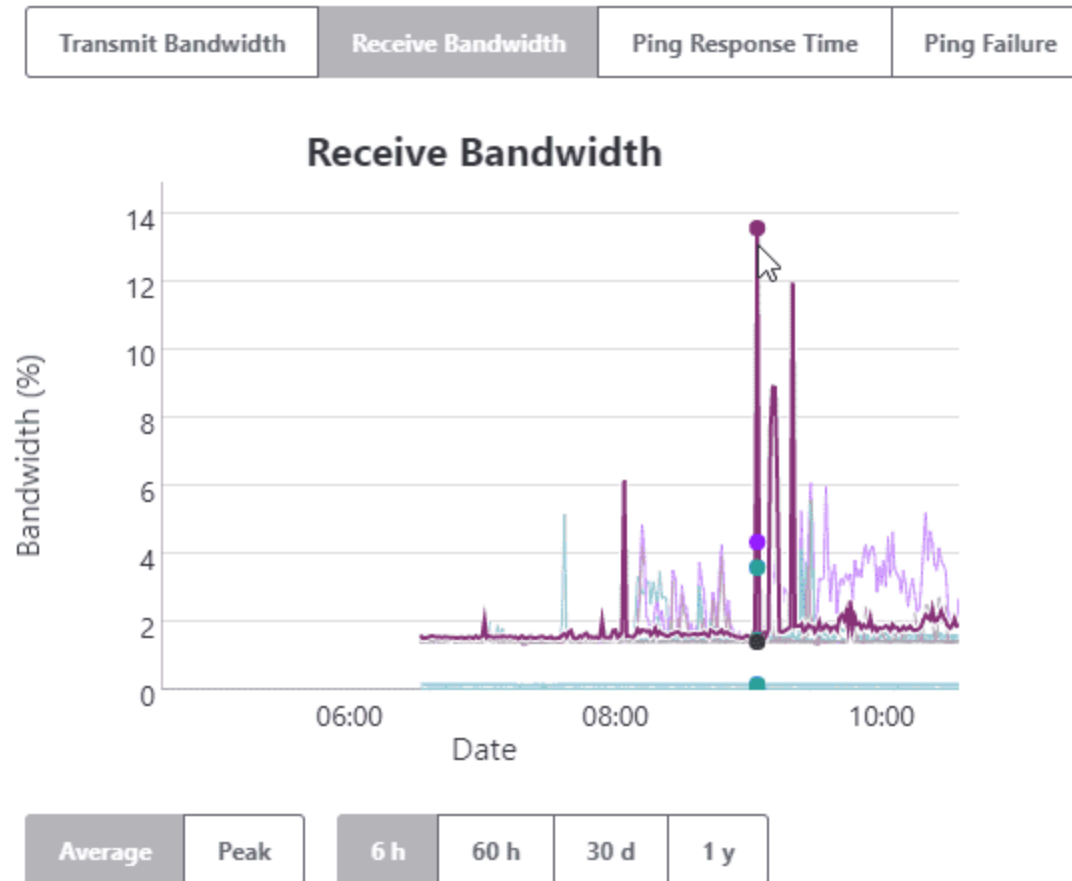


Figure 14. Sent data by source device according to Transmit Bandwidth graph.



Jun 2, 2015 9:04 AM:  
**10.1.1.171 - Dell Managed Switch:** 0.0398952  
**10.1.1.137 - EthernetSwitchArea1:** 1.47522  
**10.1.1.188 - N-TRON Managed Switch:** 4.34171  
**10.1.1.175 - Cisco Managed Switch:** 2.50067

Figure 15. Received data by target device according to Received Bandwidth graph.

This data is also provided in the Diagnostic report so that the details are quickly identified without having to analyze and charts.



**Point to Point traffic:** *The following end devices had simultaneous bursts in transmitted and received traffic that exceeded 40% bandwidth in the last 60 hours. This could be a large file transfer between these two devices.*

Between 2011-09-13 16:17 and 2011-09-13 16:22		Transmit	Receive
10.1.1.92	dim1100.i-vue.com	69.6	1.8
n/a	Auto Inserted Node (port 6 of 10.1.1.136)	1.7	70.6
Between 2011-09-13 16:53 and 2011-09-13 16:55		Transmit	Receive
10.1.1.92	dim1100.i-vue.com	76.4	1.9
n/a	Auto Inserted Node (port 6 of 10.1.1.136)	1.9	77.4

Figure 16. Same graphs as above are automatically reported in the "Point-to-Point Traffic" section of the Diagnostic Reports.

### Bad RSTP, Ring Switches, or accidental cable loops

IntraVUE continually communicates to the managed switches obtaining details how the switches are seeing the location of the devices. The communications occurs once a minute in which data from the switches Bridge MIB is accessed. This information is used to provide an accurate mapping of the interconnections of the network. IntraVUE is not a wiring diagram (however in most simple cases it represents the actual wiring) but represents what port the switch will use to send traffic to a specific device (Figure 17). This is the heart of the mapping capability of IntraVUE which also contains many rules and exceptions to deal with more complex architectures.

**Device Moves:** *Reporting devices which moved in the last 30 days which are admin verified and not enabled for automatic moves.*

*Configuration Note: If any of these devices are allowed to move, the IntraVUE administrator should check the Auto Connect checkbox in Device Configuration.*

10.1.1.49	
2011-09-13 09:48:59.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 192.168.200.174:21
2011-09-13 09:51:20.0	Device 10.1.1.49 moved from 192.168.200.174:21 to 10.1.1.136:2
2011-09-13 16:51:36.0	Device 10.1.1.49 moved from 10.1.1.136:2 to 10.1.1.171:49
2011-09-13 16:54:31.0	Device 10.1.1.49 moved from 10.1.1.171:49 to 192.168.200.174:21

Figure 17. Diagnostics Report shows the source and destination IP Address and port number.

Occasionally the ability to have a single and consistent path for the switch can be interrupted. This can be caused by a number of issues such as a loop back wiring, momentary link losses on a RSTP and Ring, or the switch being confused by MAC addresses that are too close in number. In these cases the IntraVUE may oscillate between to links or report MAC addresses on two different ports. These disturbances will be logged in the event log and may also be seen as the network changing in the main IntraVUE display. In this the IntraVUE is trying to accurately represent the network that is constantly changing.

### Resetting Switch or Switch Failing

It is important to identify if a problem is application or network related. In one case a switch was having difficulty and doing a periodic reset. This is not uncommon with older switches. Many are configured to reset if their cash memory reach certain levels. Others may reset based on a poor power connection. Whatever the case the reset may create a momentary disruption in data transmission (Figure 18).

Figure 18. A sample of a switch failing.

IntraVUE trends the transmitted and receive data on a time line and below trend the ping response time and ping failure percentages below. This graphing can provide graphic evidence of the drop off

of communications at the same time the ping failures go to 100%. The time basis also provides some clues to research to determining what may be happening with the switch at that time.

### **Overloaded or misbehaving devices**

Automation networks contain many devices from several different manufactures. This diversity coupled with the ages of some of the equipment will mean at some point devices will start to have problems. One method to determine if a device is starting to have problems is a delay in the ping response time. By measuring the response time (Figure 19) continually IntraVUE can have a means to determine if there are any relative issues that may be represented as a change in normal response times.

Figure 19. Ping response time measured for all devices in the map view.

By selecting all devices in a graph you can use it to see if an event has caused a group of devices to experience an increase in response time. This can help identify what devices were affected.

Figure 20. Multiple devices experience a delay at the same time.

**Ping Response time issues:** *Reporting devices having periods in which the ping response threshold exceeded for 2 or more consecutive minutes in the last 6 hours of scanning. Reported devices could be overloaded or having internal issues. They may be devices which should have their thresholds increased from the default, like wireless devices.*

*Note: In the future, connection issues may be broken into classes such as consistent and intermittent.*

IP Address	Name	Threshold	Avg	Max	Minutes	Over	Conseq Over
10.1.1.244	Cisco_Switch	30.0	16.3	158.3	359	73	14
10.1.1.252	cisco2950switch	30.0	17.3	191.4	359	83	18
10.1.1.58		30.0	7.5	935.7	285	18	14
10.1.1.160	oldlinux	30.0	6.2	191.3	359	25	2
10.1.1.136		30.0	9.1	84.1	359	45	4
10.1.1.234	CS-IV MINI 4.0	30.0	16.2	260.4	359	62	11

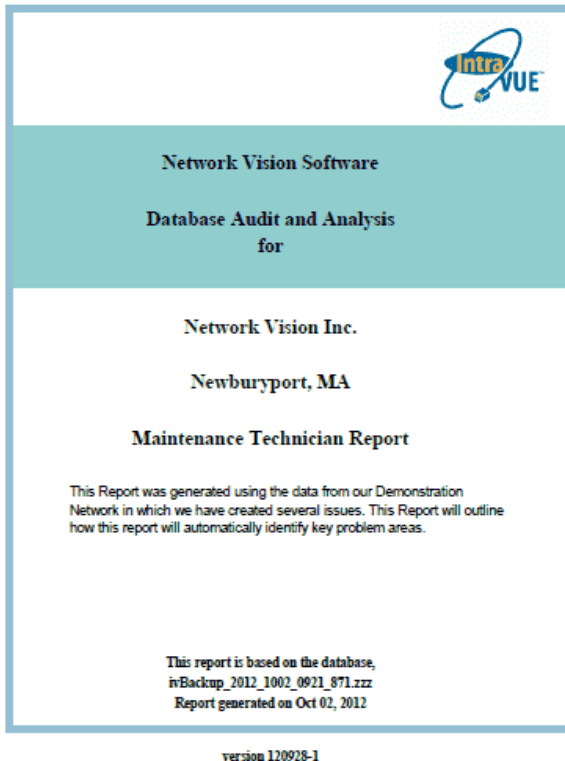
Figure 21. This is also shown in the Diagnostics Reports.

The IntraVUE solution uses the data being collected for a variety of methods of interacting with individuals. Support of the automation networks may be shared between maintenance technicians, control engineers, and IT or network professionals. Each may have a different level of skill and interest. IntraVUE provides a variety of methods as a means to focus on the issues relating to each and delivers information in a variety of forms.

### Basic Diagnostic Reports

This has been referenced in the above as a way to provide analytical results based on our methodology. There will be a variety of reports to match the intention of the user. Visit <http://www.panduit.com/intravuesupport> for more details.

- ⌚ Maintenance reports will provide analysis of the issues occurring on the network
- ⌚ Asset Reports will provide a spreadsheet with the key data such as device details and switch port location.
- ⌚ Configuration Reports will help with the configuration of the IntraVUE system



### Live IntraVUE Screen

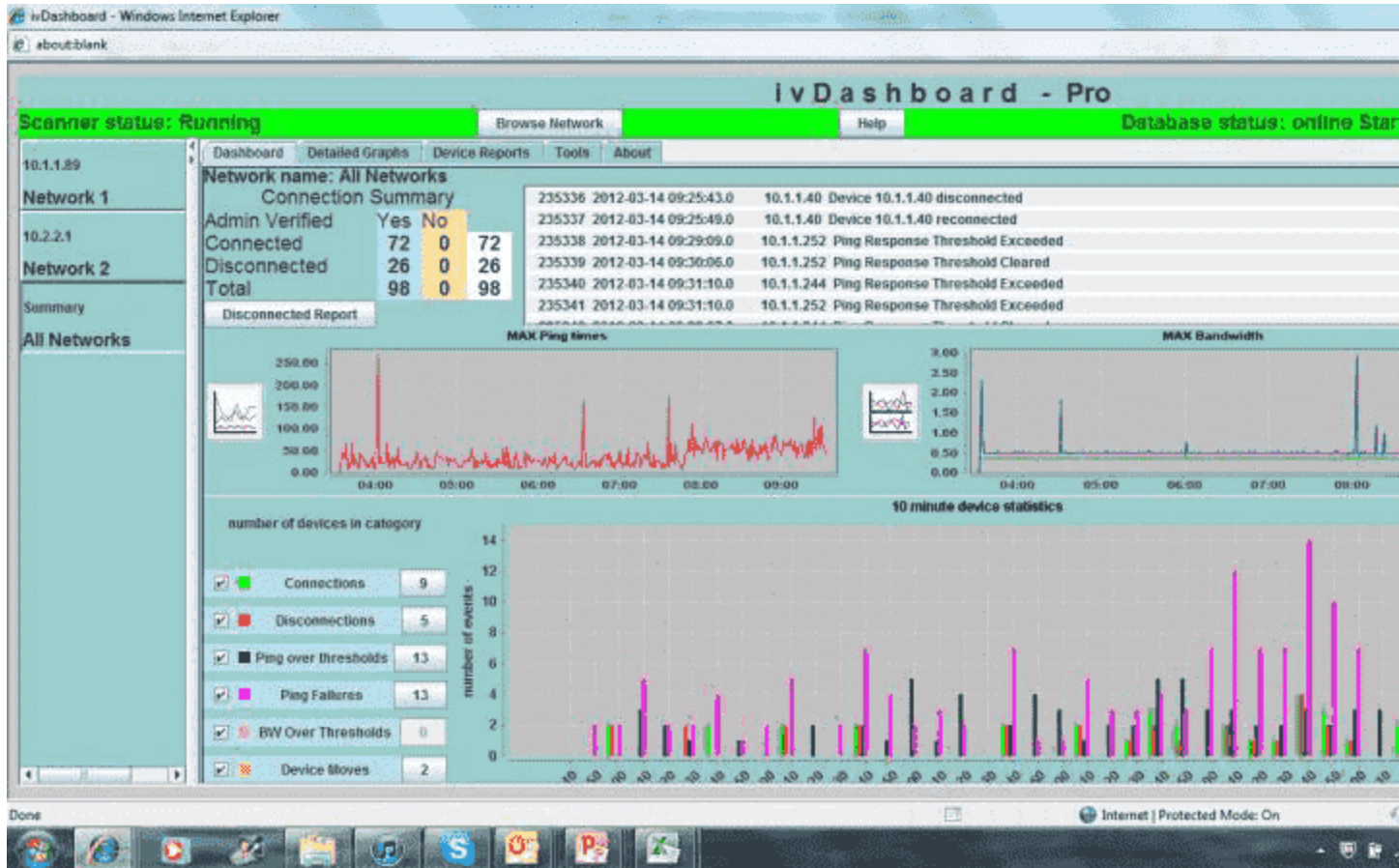
IntraVUE provides a live animated graphical view that can be view from any computer browsing to the IntraVUE system. IntraVUE provides links to pop up windows that have been review in the above material.

This view is used by maintenance technicians and control engineers to quickly identify and resolve basic problems.

### IntraVUE ivDashboard

The IntraVUE™ ivDashboard provide more experienced users with a way to associate the data collected in ways to help better review complex issues. It allows greater association of the devices with the switches as well as the inter relationships of the networks. The ivDashboard is used by Control engineers and Manufacturing IT people.

The ivDashboard tab shows detailed device statistics over the 6 hour period that IntraVUE™ maintains one minute resolution threshold data.



The upper part of the ivDashboard tab shows a Connection Summary and the last 10 events for this IntraVUE network. The data is automatically refreshed several times a minute to get new events and to update the connection data.

In the center of the ivDashboard panel are two graphs which show the maximum data point for each threshold for any device in the network. Based on what you learn as being 'normal' for a network, you should be able to spot changes from 'normal'.

The 10 Minute Statistics, at the bottom of the dashboard, provide an instant, visual indication of what is happening in the selected IntraVUE network.

On the left, each of the 7 statistics is listed with its color code. The checkbox at the far left determines if that statistic will be graphed. The setting is persistent when changing networks.

While the graph shows how many instances of the statistic occurred over the 6 hours, the number next to the statistic on the left tells you how many different devices caused the statistic. Its possible only one device caused a large number of disconnections or ping failures. In the image above, 6 different devices caused the 6 ping failures that occurred.

All three graphs have the option to be printed. Right click in the graph area and you will get the print option.

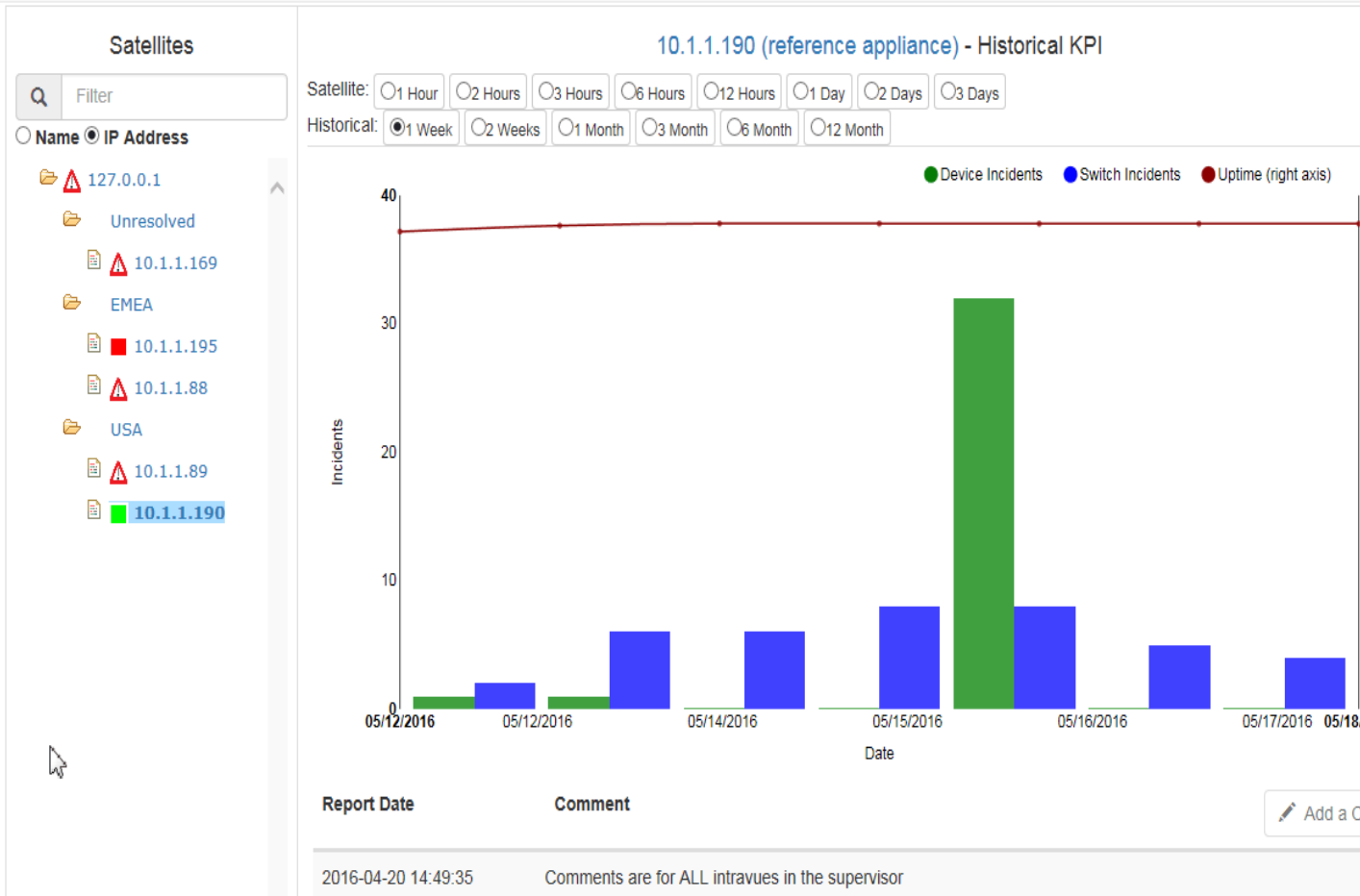
The ivDashboard comes with its own help.

The ivDashboard is compatible with IntraVUE™ 3.

Your License Product Key will let IntraVUE™ know if you have the ivDashboard feature (i.e. if you're an Advanced Subscriber).

See Downloads to get the latest version.

## IntraVUE Supervisor



The IntraVUE™ Supervisor is used in large installations where many distributed IntraVUE systems are deployed. This can be in either a single large installation or a central support group supporting many different plants. The Supervisor monitors not only the health of the networks but also of the IntraVUE systems. It provides the ability of a single individual to oversee hundreds of IntraVUE systems and potentially thousands of networks easily.

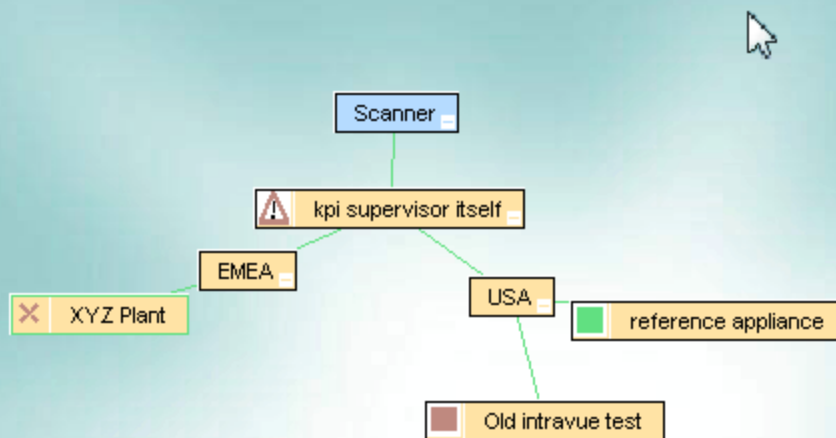
See [KPI Supervisor \(IntraVUE™ Advanced Analytics\)](#)



## KPI Supervisor (IntraVUE™ Advanced Analytics)

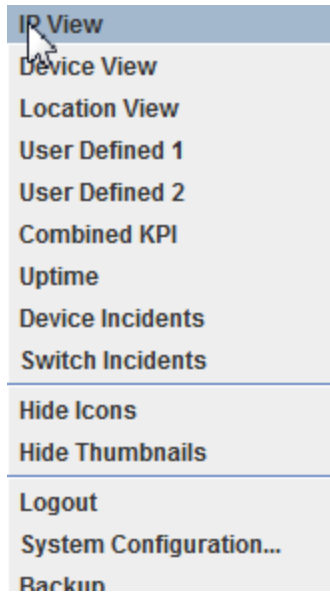
The KPI Supervisor (Included with advanced subscription) replaces the previous versions of the Supervisor. It provides a centralized manager of other IntraVUE™ servers using the familiar map interface to graphically represent each remote instance. The KPI Supervisor uses the KPI data in the remote satellites to display a 'state' and to provide statistics in additional graphics.

### Combined KPI



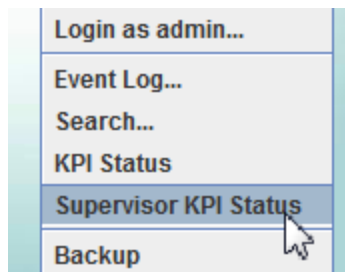
The locations of the satellite servers we made using the Add Child function to create the EMEA and USA nodes, and then the appropriate satellite was manually moved to the right location.

The KPI Supervisor renames the user defined 3, 4, 5, and 6 views to Combined KPI, Uptime, Device Incidents, and Switch Incidents.



In each one of these views the icon will represent the current threshold state of the selected incidents or uptime. In the Combined KPI view, the worst case icon is used. See Configuration for how to set the threshold values for each. Red, Yellow, and Green icons represent known states and other icons represent failure to connect, the satellite database is not current, etc.

In order to use the KPI Supervisor and access configuration and reports, select Supervisor KPI Status from the System Menu.



The KPI Supervisor package only comes with the advanced subscription of IntraVUE™.

See [here](#) for more details.

[Installation](#)

[IntraVUE™ Key Performance Indicators](#)

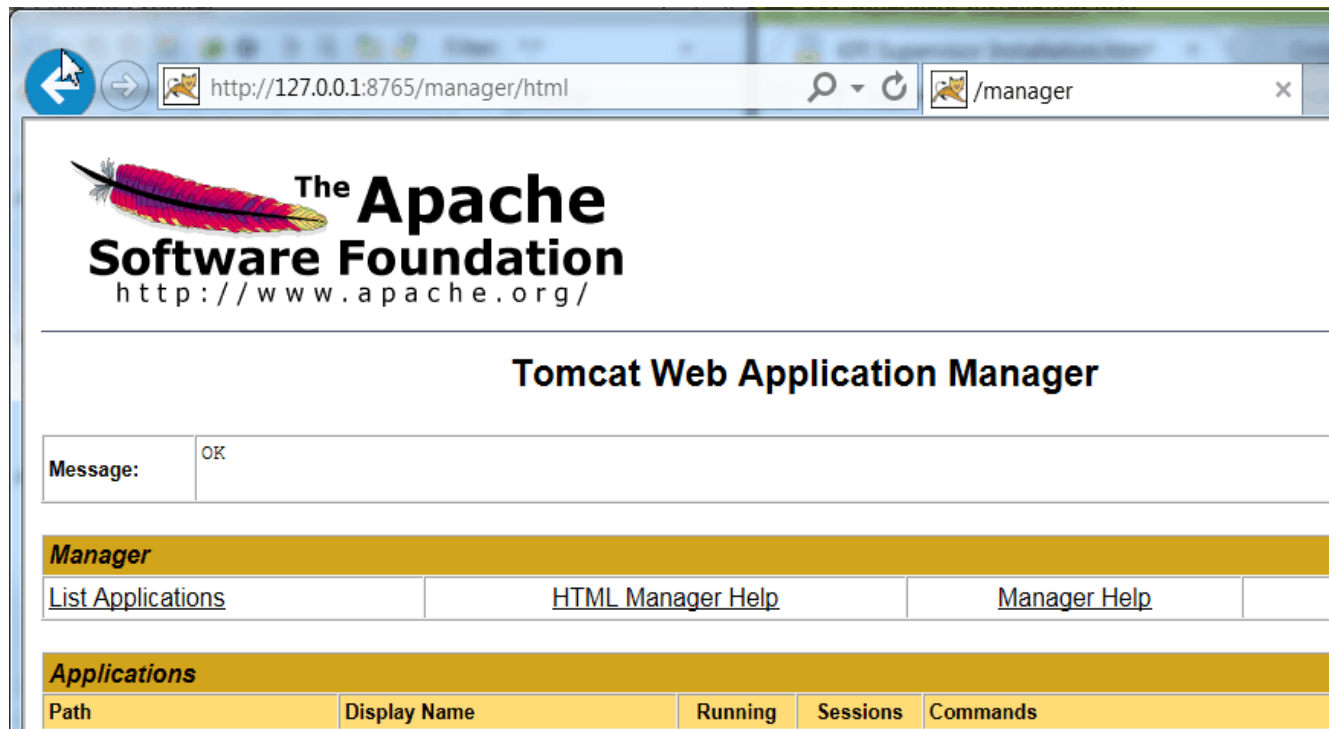
[KPI Supervisor Configuration](#)

## KPI Supervisor

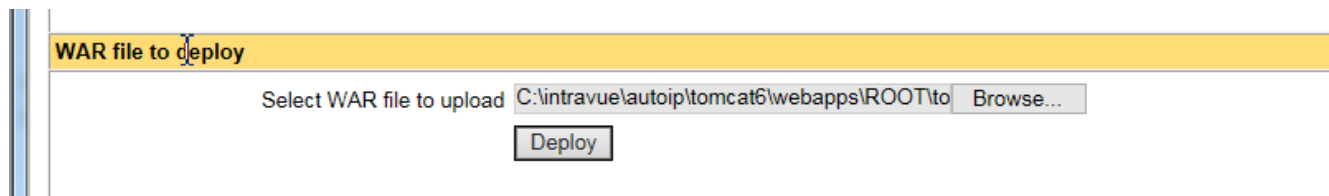
## Installation

Installation of the KPI Supervisor is done after installing the basic IntraVUE™ installation.

1. Open the web application manager with your browser using `http://ip-of-intravue-server-:8765/manager/html`. Enter 'admin' as the user and the IntraVUE™ password.



2. Go to the bottom of the web page and find the War File to Deploy section. Browse to and select `...\IntraVUE™\autoip\tomcat8\webapps\ROOT\tools\superkpi.war`.



3. Then click on 'Deploy'. The browser will move to the top of the page and you will see an OK message when complete.
4. After deploying the KPI Supervisor, the Scanner tab of System Configuration will be disabled.



All configuration of the Key Performance Indicators is done in the [IntraVUE™ Key Performance Indicators](#) page.

## IntraVUE™ Key Performance Indicators

There are 3 Key Performance Indicators (KPI) maintained by IntraVUE™.

1. Uptime for critical devices meant to be on all the time
2. Total incidents for Devices
3. Total Incidents for Switches

Incidents are certain events in the event log such as device disconnects, ip or mac address changes, and over threshold events.

Every device has one of four critical states assigned

- » Unknown, the default, means no one has made a determination of this devices state.
- » Ignore - the device is not critical to production or operation
- » Critical Intermittent - the device is critical but sometimes is not available. For instance a switch inside a robot cell where all power must be removed to the cell before a technician can enter the cell.
- » Critical Always On - the device is critical and uptime should be measured and reported.

Ideally, there will be no Critical Unknown devices or only for newly discovered devices.



Refer to for settings location and how to configure them for multiple devices in bulk.

All configuration of the Supervisor is done in the [KPI Supervisor Configuration](#) page.

## KPI Supervisor Configuration

After logging in with the same password as IntraVUE™ you can add and remove devices from being supervised by selecting Configuration.

To add a satellite you can select an existing one and modify the IP and name or you can enter it from empty fields.

An email address can be added for each remote satellite, More than one can be added with commas and NO SPACES.

Email must be enabled in the main System Configuration's email tab with the service correctly configured.



Category	Percentage
No	25%
Yes	50%
Don't know	25%



The color of the icon in the map view of the Supervisor is set according to the percentages set in the configuration screen. Additionally if you want to have email notifications you can change the Notification buttons to the right of each type of KPI to the appropriate color.

The red X next to each satellite will delete it after a confirmation.

An icon to the left of each satellite indicates its current Combined KPI state set by the sliders in the configuration dialog.

- Current Combined "Best" KPI state or good communication

- Current Combined "Average" KPI state or okay communication

- Current Combined "Warning" KPI state or degraded communication

- Current Combined "Worst" KPI state or bad communication

- Satellite disconnected. Responds to ping, but does not respond on port 8765 to Standard KPI request

(Could be non-IntraVUE device or IntraVUE with no Standard KPI)

- Red Exclamation Triangle - Indicates a problem (see below)



**Black X** - device is defined in supervisor but has not been found on the network

Problems include:

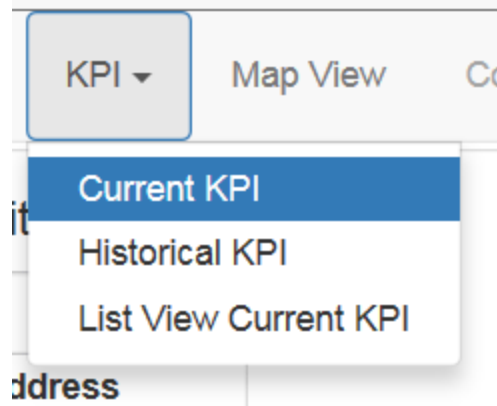
- » No connection to the satellite
- » Connected satellite IntraVUE™ is not running.
- » Satellite does not have a version of the software that supports the latest version of KPI or no KPI devices have been configured.
- » No devices are set to a KPI status that is not 'unknown' in the satellite.

All configuration of the Supervisor is done in the Configuration menu.

## KPI Supervisor Reports

## Current KPI View

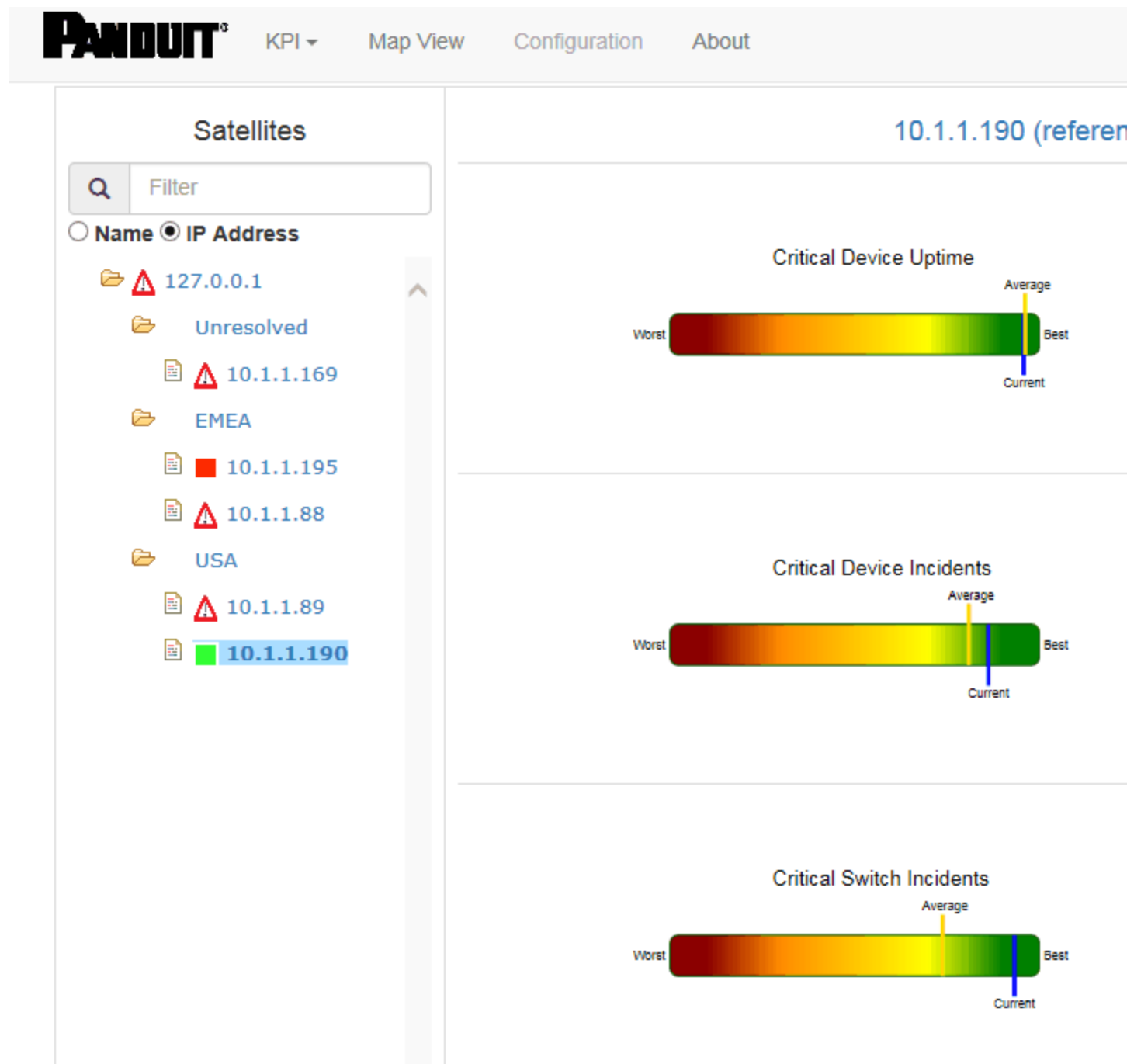
The 'KPI' menu item provides access to the 3 main status pages.



The Current KPI page compares the KPI statistics from the last 24 hours to the statistics from the last 30 days.

Each colored bar represents a range of data. The left side of the bar is the worst value in the last 30 days, the right side is the best value for the last 30 days. The actual values are displayed to the right of the bars as well as the date/times those occurred.

The yellow bar shows where the 30 day average is located between the worst and best days. The blue bar shows where the last 24 hours compares to the worst and best days. The position of the yellow and blue bars indicate if the KPI values are improving or not.



On the right are the actual (msec) values used in creating the bar charts as well as telling you when the best and worst days were.

To see the statistics for a satellite, select the IP address or name of the satellite on the left side. A radio button allows you to change between those views.

An icon to the left of each satellite indicates its current Combined KPI state set by the sliders in the configuration dialog.

- Current Combined "Best" KPI state or good communication

- Current Combined "Average" KPI state or okay communication

- Current Combined "Warning" KPI state or degraded communication

- Current Combined "Worst" KPI state or bad communication

- Satellite disconnected. Responds to ping, but does not respond on port 8765 to Standard KPI request

(Could be non-IntraVUE device or IntraVUE with no Standard KPI)

- Red Exclamation Triangle - Indicates a problem (see below)



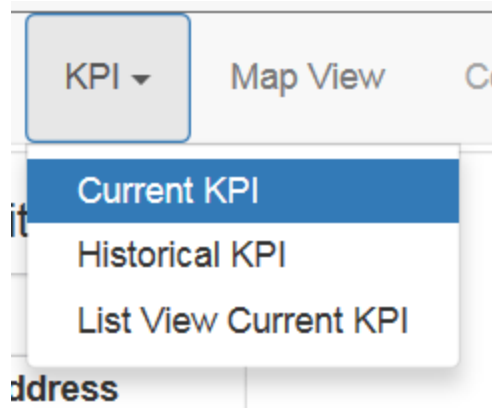
**Black X** - device is defined in supervisor but has not been found on the network

Problems include:

- » No connection to the satellite
- » Connected satellite IntraVUE™ is not running.
- » Satellite does not have a version of the software that supports the latest version of KPI or no KPI devices have been configured.
- » No devices are set to a KPI status that is not 'unknown' in the satellite.

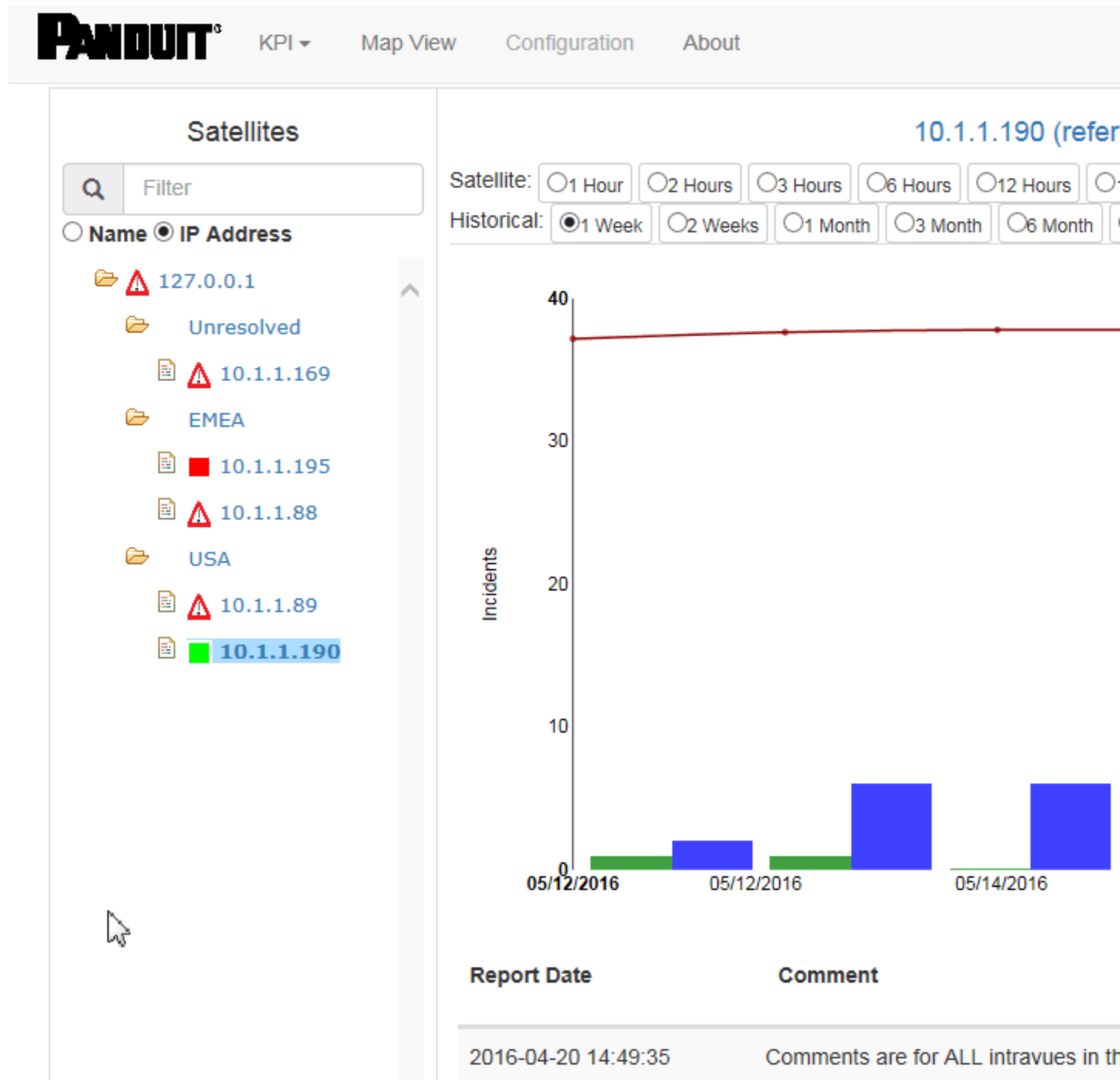
## Historical KPI View

The Historical KPI view is selected from the KPI menu item.



The Historical KPI chart shows the daily total device incidents, switch incidents, and uptime percentage for many time periods up to 1 year.





On the left of the graph is the scale for device and switch incidents. On the right is the scale for uptime.

At the top of the graph you may select which time period you are interested in viewing, from 1 hour to 12 months.

An 'Add Comment' button allows the user to enter comments to document or describe any unusual conditions. The comments will be displayed below the graph. See

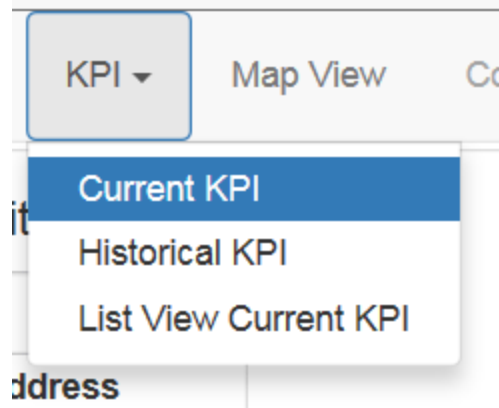
Selection of satellites and the color coding to the left of each satellite is as described in the Current KPI page.

Details on the data used for various periods



Period	Data
1 hour, 2 hours, and 3 hours	values are based on 2-minute intervals
6 hours, 12 hours, 1, 2, and 3 days	values are based on 1 hour intervals
1 week, 2 weeks, 1 month, 3 months	values are based on calendar days
6 months and 12 months	values are based on calendar months.

## List View

The List View is selected from the KPI drop down menu.



The List View provides a high level summary of each satellite and has columns for data from the satellites. Each column can be sorted in ascending or descending order.

<div>  <div> KPI ▾ Map View Configuration About </div> </div>										
<div> <div>  Filter </div> </div>										
		Device Count		Critical Device Uptime				Critical D		
Name	IP Address	Non Admin Verified	Unknown Critical Status	Current (%) ▲	Critical Device Count	Min (%)	Max (%)	%	Normalized	C
✖ XYZ Plant	10.1.1.195	— / —	— / —	36.64	293	0	92.9	—	—	0
■ Old intravue test	10.1.1.89	— / —	— / —	67.73	22	61.05	67.77	—	—	0
■ reference appliance	10.1.1.190	144 / 152	89 / 152	83.77	50	81.65	93.85	0.79	0.03	5
⚠ kpi supervisor itself	127.0.0.1	4 / 4	2 / 4	100	2	99.99	100	50	2	2

The **Name** column also contains an icon as described in the previous pages. It reflects the icon that is used in the 'combined KPI' view.

'**Non Admin Verified**' shows the number of devices which are unverified and the total number of devices.

'**Unknown Critical Status**' shows the number of devices which have not been set to the Ignore, Critical Intermittent, or Critical Always On states, as well as the total devices.

The **Critical Device Uptime** columns show the current uptime (for the last 24 hours) as well as the lowest and highest percentages for the last 30 days. The Critical Device Count is the count of all devices set to Critical Always On.

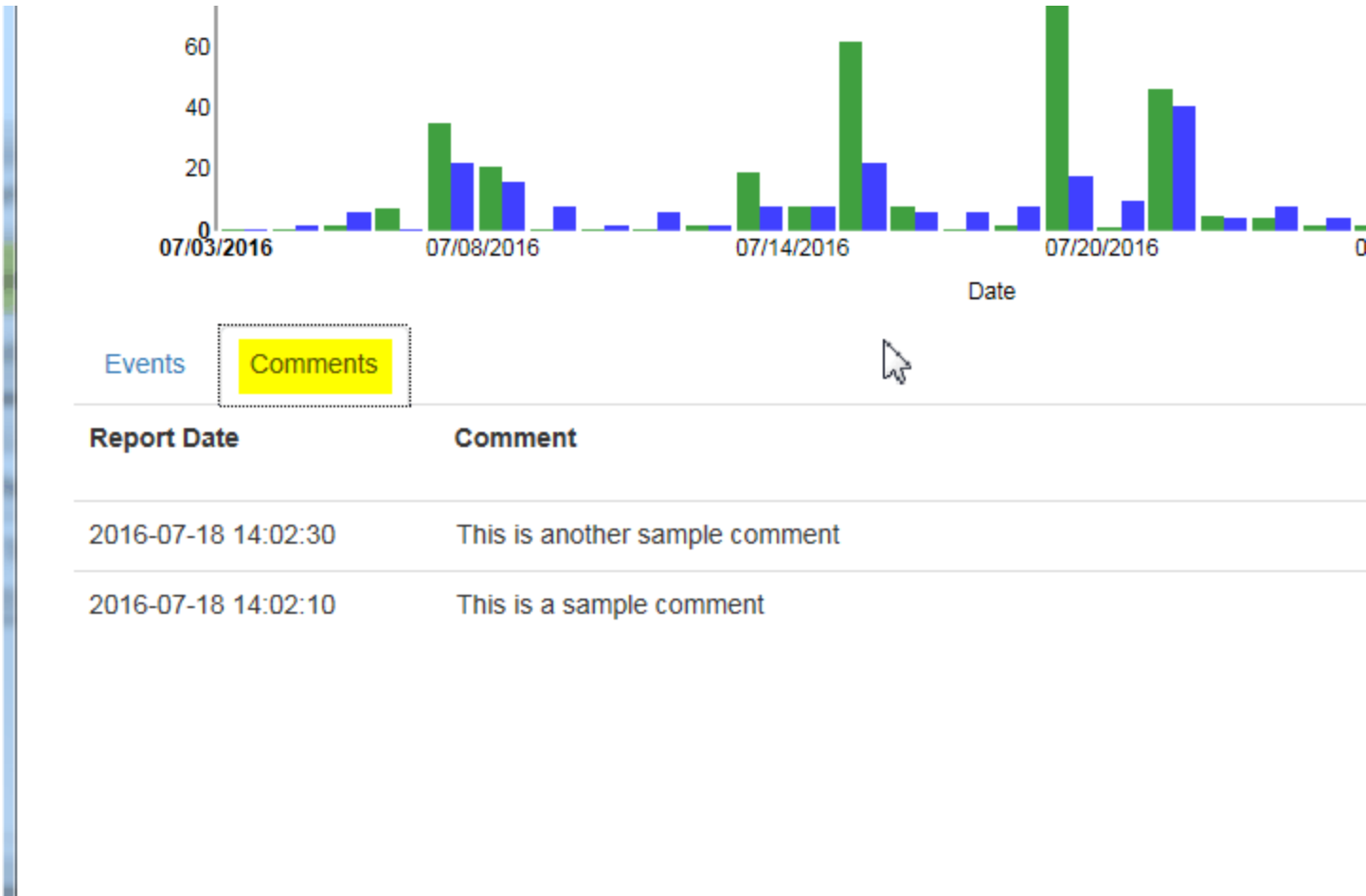
The **Critical Device Incidents** and **Critical Switch Incidents** section each have several columns.

- » The '%' column is where today's incidents are compared to the worst and best for the last 30 days.
- » The normalized column shows the number of device or switch incidents divided by the number of devices or switches. It can be thought of as the KPI value for that statistic.
- » A 'Count' column shows the number of devices or switches that are set to Critical Intermittent or Critical Always On.
- » Additionally there are columns to show the current number of incidents in the last 24 hours, and the minimum and maximum number of incidents in any one 24 hour period. The '%' column shows where the current value is compared to the minimum and maximum.

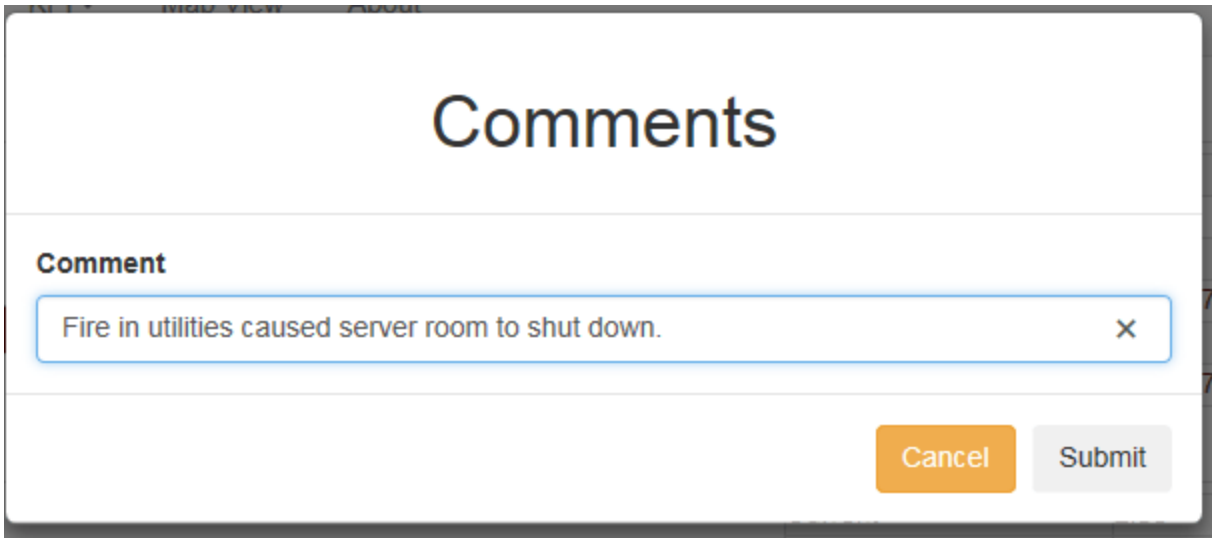
## Adding KPI Comments

The KPI module allows the user to add comments that will appear in both the IntraVUE™ event log as well as the KPI reports. You must be logged in as a KPI administrator to add a comment.

In the bottom portion of both the Daily and 30 Day KPI pages you can select viewing of Events or Comments.



To add a comment, select 'Add a Comment'



The screenshot shows a modal dialog box titled "Comments". Inside the dialog, there is a label "Comment" followed by a text input field. The input field contains the text "Fire in utilities caused server room to shut down." and has a small "x" icon in the top right corner for clearing the text. Below the input field, there are two buttons: "Cancel" (orange) and "Submit" (gray).

Enter the comment text. The date / time of the comment will be the same as when it was created. The comment will also appear in the main IntraVUE™ event log.

## Additional Resources



## Technotes

## Keeping Track of Port Speeds

Ethernet communications between automation devices and switches can occur at different speeds. Older equipment may only operate at 10 MBPS, while newer devices operate at 100 MBPS, and Computers can communicate at Gigabit speeds. Switches provide the flexibility and buffering so that communications between two devices can occur even with different connection speeds. This can also be aggravated by the various ages of equipment and their different communication capabilities. These speeds can either be automatically established by negotiations between the switch and device or manually set.

Choosing manual or auto-negotiations may depend on the device and application. Other considerations for speeds may be due to quality of the connection and its susceptibility to noise, reflection, or other interference.

It is useful to know the current speed of the connection as well as if the connection is changing speeds due to the issues stated above. IntraVUE now provides an easy method to view the current connection speeds as well as logging any changes in speeds to help in troubleshooting connection problems.

In order to determine the speed at a connection with IntraVUE, simply right click on the connection. A window will open with connection details that will include the Link Speed. This is seen on the top line in the picture below. If the device is connected to an unmanaged switch as seen in figure 1B but has SNMP enabled, the speed details will be obtained from the actual device. IntraVUE will display the source of the data as seen in the two pictures below.

Figure 1A: Link Speed Data from the managed switch

Figure 1B: Link Speed Data from the Device via SNMP

IntraVUE will record the initial port speed and any changes to the speed over time. This can be very valuable information in the identification of any changes in speeds that typically indicate either a problem connection or poor quality signal. Many of these issues that may affect port speeds may not have a severe effect on the application. Performance may degrade and recover before there can be any analysis for the location and reason for the slowdown in performance.

Upon the initial discovery of a switch the ports will be reported as going from 0 to their current speed. Only the active Ports that are connected to the devices in the IntraVUE scan range will be shown on a per network basis.

Figure 2: Initial discovery of the port speeds on a switch in the Event Log

Speed changes by connection will also be displayed in the event log. Anytime a change of speed is reported it will be recorded with the date, time, and change in speed. These will appear with other events being logged by IntraVUE. In order to filter for only the speed events you can place the word “speed” in the Additional Text Field and only speed events will be displayed.

Figure 4: Filtering for all speed changes in the IntraVUE Event Log

Adding the specific speed change in the text field you can filter the entire database to find changes, ie; going from 100 to 10 MBPS or from 10 to 100 MBPS can filter and look for specific speed changes and the frequency of the changes. Using 1000 would identify if any communications were taking place at Gigabit speeds.

Figure 5: Filtering for speed changes from 100 to 10 MBPS in the Event Log

Once a connection is chosen you can adjust the filtering which will add the other events for this specific device such as SNMP communications, ping failures, ping response times, and bandwidth issues. This may provide addition details of the effects on the device during a speed change.

Figure 6: Filtering for all events for a device during a speed change

Selecting the switch and the connected device in the IP Address Filter will provide a means to obtain specific details that can provide potential reasons for a speed change.

## Identifying Auto-Negotiation issues

The use of IntraVUE to identify auto-negotiation problems can eliminate one of the major causes of intermittent disruptions on the network. If a connection is lost or if the signal quality should degrade, switches that are set for Auto-Negotiate will try to establish communications by switching speed and duplicity. This may reduce communications from 100 MBPS to 10 MBPS and the available bandwidth used on the connection will increase 10 fold for the same communications. This can be seen in Figure 7B.

Figure 7A: Events surrounding a speed change

Figure 7B: Trend graph with an increase in Bandwidth and ping failures

## Conclusion:

The addition of monitoring and graphing the Port Speeds will provide another key capability that will help individuals identify subtle issues that can effect performance and interfere with real time applications. Any device having both ping failures and Port Speed changes should have the configuration of the device and the port of the switch reviewed. These details will also be used for our Diagnostic Reports and Network Health Status, which will help individuals that are not Network Experts deploy and support equipment communicating over Ethernet.

# Understanding Spikes In Networks

One issue that can affect the performance of an automation application is when the network receives a burst of traffic that interferes with real-time data flow and creates application problems or lockups in automation devices. These disturbances may only occur for a short period of time, but can stop devices from communicating as they are not able to recover from the burst. By the time you can run network sniffers to analyze the problem it may be too late to capture any real details. One may be left hoping that the problem reappears when you are ready to capture the disturbance.

IntraVUE has proven to provide graphic proof of spikes in traffic and will help determine if the issue is a point to point Unicast burst, or a Multicast/Broadcast and the devices that were affected. Many switches are able to throttle these bursts and it may only be the local switch that is affected. IntraVUE provides a method that identifies many of these incidents and the data is stored so that analysis can happen hours after the occurrence.

## Live Graphical View

IntraVUE's graphical view changes from green (healthy communication) to yellow (parameter exceeded) when the traffic on the link exceeds a preset limit.

The picture below provides a quick view of two devices establishing communications that have exceeded the limits set. In this example a contractor connects to a switch and downloads a large configuration file to a drive system. In the process the link between the N-Tron switch and a Dell Switch also exceeds its limit that has affected devices below the N-Tron switch which are reporting information to SCADA systems upstream of the switch.

IntraVUE showing two devices with a large data transfer

The graphic below shows all the ports on a switch in an alarm level. Broadcast traffic problems can over-run all the ports on a switch and flood all the connected devices with unwanted traffic. In addition the 10.1.1.142 device stopped communications as a result of the overload.

Yellow lines can be due to traffic exceeded or Ping response times exceeded as the switch shuts down port traffic.

Apparent broadcast storm on a Cisco switch

When the Broadcast storm ends and the switch and its links recovers however, the 10.1.1.142 remains disconnected. If one is not looking at the display during the time of the disruption, you would see only the device disconnected but no visual indicators in the display. IntraVUE however has stored all the events in the event log and can display a trend of the data to easily provide details of the past event.

Broadcast Storm ended but a device did not recover

Viewing a disruption that has occurred in the past

IntraVUE captures the details of the network parameters and stores the data in a relational database. Selecting the disconnected device and choosing the Event Log you are able to see that several devices had exceeded transmitted traffic prior to disconnecting.

Expanding the event log to include all devices at that specific time will provide additional details of the devices affected and the ports that carried the excessive traffic. Many of the affected devices that had lost connection were back online. Only one device was unable to recover.

The Event log provides a method to look at a time based “cause and effect” that can help provide necessary details for solving the problem.

In addition to the Event Log to identify the time and devices affected, IntraVUE provides Trend Graphs that provide additional methods of viewing the collected data. It can provide a way to determine if the excessive traffic was “point to point” Unicast or “one to many” Broadcast or Multicast.

Trend Graphs for Bandwidth Data

The time based trend graphs provide another visual for assisting in the analysis of excessive traffic. The Trend Graph allows the selection of a specific parameter such as Transmitted data or Received data. You can also choose to look at this on a specific switch or a larger area including the entire network. By looking at the results of both Transmitted and Received you are able to link the connected devices.

Large File transfer between two devices can easily be seen from the displays below. The display shows at two separate times there was a large data exchange between the two devices.

If there was a single device transmitting to many devices at the same time it would most likely be caused by a Multicast or Broadcast. In the figure below 10.243.38.224 generated an unusual level of traffic exceeding 50% of the available bandwidth and at the same time many devices reported a spike in receive traffic.

These trend graphs provide additional details to enhance the data provided in the Event Log. This information can be easily obtained by using the various screens available in IntraVUE. If the individuals responsible for support require additional assistance to help identify these problems, IntraVUE provides the ability to take the recorded data and send it electronically to a diagnostic report generator in which a written PDF report is sent to targeted individuals via email with details.

IntraVUE Diagnostic Reports will contain a section that highlights these two types of events in the PDF that will makes it easier for the local resources to understand the problem and the devices affected.

IntraVUE provides a variety of ways to help you identify burst of traffic that can occur and create problems for automation systems. The recorded data means that these intermittent issues will not require your constant attention. This is just one of many capabilities which makes IntraVUE the solution for automation people supporting automation networks.

## Wireless Devices Preserving Old Data

Having issues where a verified device will move to another area and keep its old data but on a new device. Such as our forklifts will be labeled properly then the next day we get on there and it is now a computer but still labeled as a forklift.

When trying to rename a device sometimes it will revert its name back to what Intravue picks it up as. If a new device is swapped out it will sometimes hold the old information on that IP address when a new device comes online to take its place.

When trying to export the data to excel it is hard to figure out which ports it is actually on because it sort of encrypts that field. Also when a laptop is connected via hardline and then goes to wireless it will keep some information but have to keep verifying it each time.

### **This problem is not common.**

The scanner makes an attempt to deal with DHCP networks, which are not normal on the plant automation side but normal in plants.

When a new device connects to the network the scanner checks to see if there is a device having the same mac address as the new device and will then move the properties of the old device to the new device and delete the old device. An event log is created to that effect.

Laptops with wireless will have different behavior depending on if snmp is enabled. If it is not enabled IntraVUE sees it as two separate devices. If snmp is enabled, the scanner will recognize they are the same device and merge them.

Some changes have been made to the DHCP software in recent versions and the handling of Network Address Translators where the same mac is used for multiple IPs may possibly play a role.

### **IntraVUE, by itself, will never forget a device.**

In a DHCP network if you delete the DHCP devices which are disconnected, IntraVUE will not have old data to transfer to the new device.

The DHCP lease time should be on the order of 3 days so a device should need to be disconnected for more than 3 days before it would get a different IP.



It would take some work to daily remove the old dhcp device(s) and perhaps that is something that could be automated in the future.

Contact support and provide a support archive and DHCP lease times to investigate this issue further.

## Limiting VLANs on Cisco Switches

To limit the vlans scanned during SNMP searches to Cisco switches, use the **force.cisco.vlans** setting in the **ivserver.properties** file.

This setting limits the vlans the scanner uses in doing SNMP to Cisco switches. When the scanner recognizes a Cisco switch by asking for the private MIB entry to list vlans, it must append an at sign (@) and the vlan number to the configured community string. The scanner must go through the complete switch query / response routine for every vlan that is configured in the switch.

When a plant is scanning 2 or 3 vlans and there are 20 to 50 defined in a layer 2 or 3 switch, it takes that many more times to complete a topology cycle.

The **force.cisco.vlans** setting provides the customer the ability to tell the scanner only use certain vlans to retrieve data.

This is a global setting and is applied to every Cisco switch scanned.

In plants with many switches, specific device / switch settings may be needed.

The **vlan:x, y, z** in the **trunkingdefs.txt** file is a method of doing just that.

It overrides the global setting and limits query / responses to that switch to the vlans listed.

## Verifying SNMP on Fully Managed Switches

Fully managed switches comply with IETF RFC 1493 and IEEE 802.1d standards. Unmanaged switches are not recommended in Industrial Network Environments.

To verify if a Layer 2/3 Switch supports SNMP and is a fully managed you can invoke the switch-probe utility to do in multiple ways:

1: switchprobe.jar - brings up the same utility as is available in Windows by going to Start / programs / intravue / tools / run switchprobe menu item. See Downloads

2: util.jsp- If you select this page you will get a list of available utilities with their syntax hints. More utilities will be added over time.

In your IntraVUE browser, substitute the URL of the IntraVUE host to be :

`http://127.0.0.1:8765/tools`

If the host resides under a different IP address, modify this accordingly.

The syntax hint must be added to the URL you use to access IntraVUE. For instance, if you access IntraVUE using "http://10.1.2.3:8765" the full URL for each of the utilities above would be:

`http://10.1.2.3:8765/tools/util.jsp?ping=10.1.2.99`

`http://10.1.2.3:8765/tools/util.jsp?tracert=10.1.2.99`

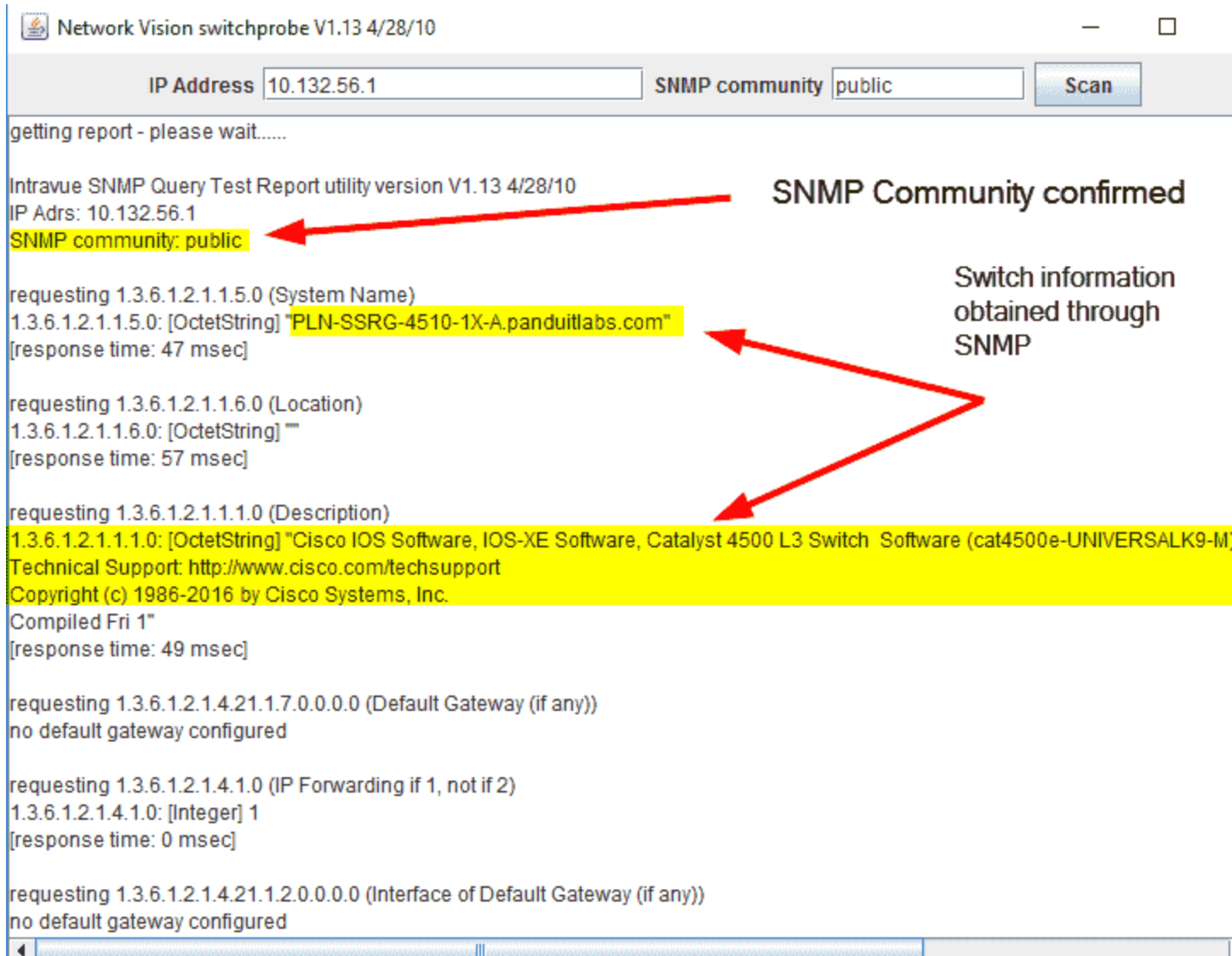
`http://10.1.2.3:8765/tools/util.jsp?switchprobe=10.1.2.99&community=public`

The Switchprobe's utility community field is case sensitive! Watch for extra spaces.

These utilities are also available on the IntraVUE Agent. After you run one of the commands, a browser window will open with the results

The switchprobe browser option allows you to use the find command to locate specific data within the switchprobe results.

3. Enter the ip address of the switch or router and the presumed community (e.g. public).



If you don't get MAC addresses and Port information that means the switch:

- A. Does not have SNMP enabled\*\*
- B. Does not have a Read-Only Community setup\*\*\*
- C. The switch is not a fully managed switch

This is what you will see when the switch or router is not a managed switch or a firewall/ACL/Antivirus is blocking SNMP/ICMP Pings

requesting 1.3.6.1.2.1.1.5.0 (System Name)

timeout - no response from x.x.x.x

abandoning further queries to this device

Usually when running the **switch probe** utility against such **switch**, at the bottom of the switchprobe results page it will return the bridge mid information with MAC address and port number for each interface of the **switch**. If it doesn't then this **switch** does not conform with either standard and can't be considered a "Fully Managed" **switch**.

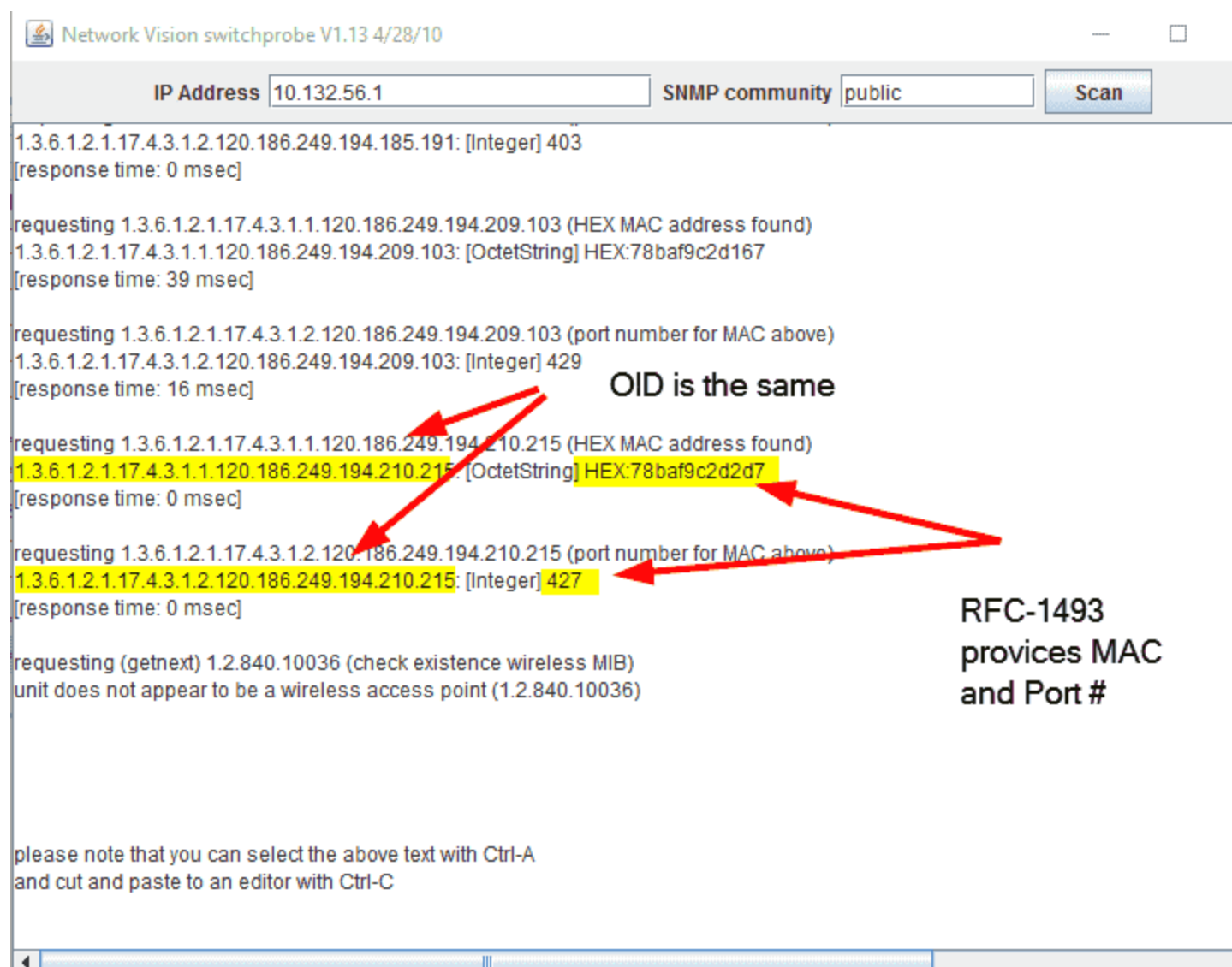
For example, this is found in a **switch probe** output for a fully managed **switch** which shows the first port found. It shows the MAC address as well as the port number for that MAC address.

...3.1.1.236..229.85.183.60.128 (HEX MAC address found)

...29.85.183.60.128: [OctetString] HEX:ece555b73c80

...3.1.2.236.229.85.183.60.128 (port number for MAC Above)

...29.85.183.60.128: [Integer] 1



\*\*Many L2/L3 switches and routers require a reboot after enabling SNMP and SNMP communities.

\*\*\*IntraVUE does not require SNMP Traps to be enabled on switches. SNMP Read-Only Communities are enough to communicate L2/L3 switches & routers in order to get MAC Addresses of end devices. IntraVUE does not write to devices.

# NA Nodes

There are two types of NA Nodes, n/a and N/A and there are subtle differences between them that would help you identify the behavior of each when you see them on the IntraVUE Map View.

### Auto Inserted n/a Nodes

Ethernet is a point to point protocol. An Ethernet cable can not be physically attached to more than one device at each end.

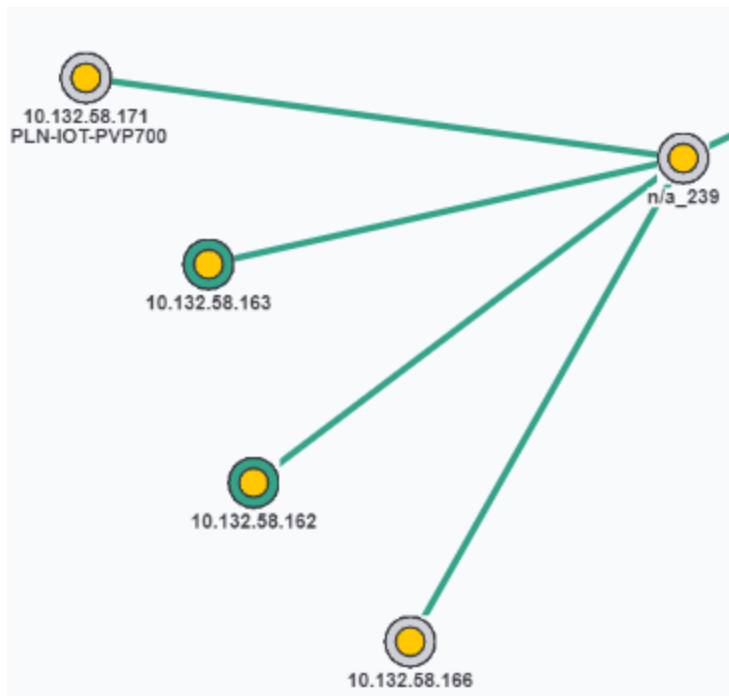
LAN traffic/packets move based on mac addresses

Switches move packets to ports based on mac address, Hubs move packets to all ports

Fully managed switches report mac addresses on each port

Anytime the scanner detects more than one mac address on the port of a managed switch that can not be resolved to a switch further down on that port, an auto-inserted node will be used to show more than one device on the port – only one line per port from the upper switch

Anytime only one mac is left on a port (because of a device move) the n/a node will be removed



### Lower case n/a nodes characteristics

Automatically inserted and removed by the scanner

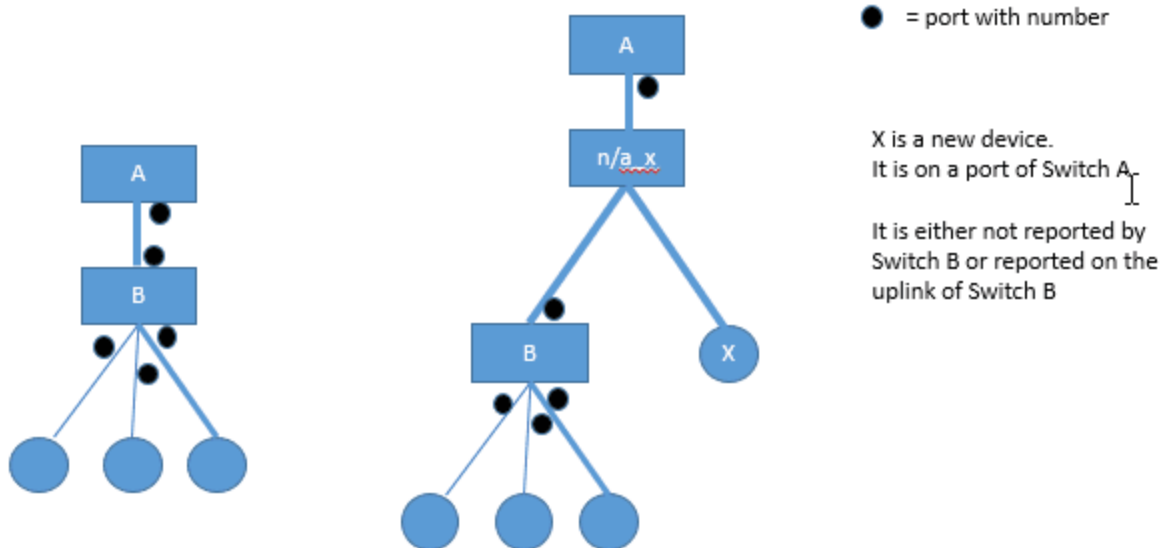
Only appear on the port of a managed switch

Represents a device which causes the scanner to see more than one mac address on a port of a managed switch

Common examples:

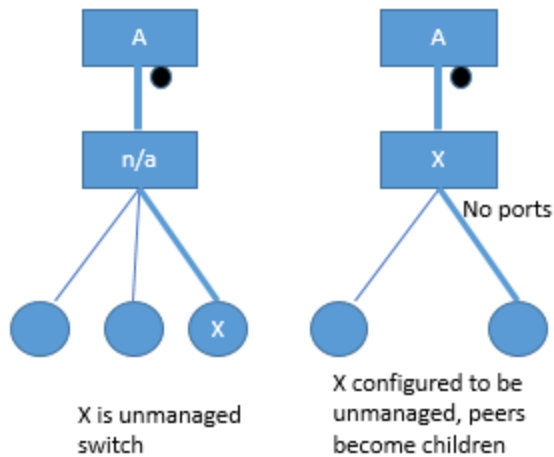
- A hub
- An unmanaged switch (fails to meet RFC 1493 standard)
- A Wireless AP
- A Hypervisor Server
- A DRL Ring (daisy-chained or linear)

## Auto-inserted node



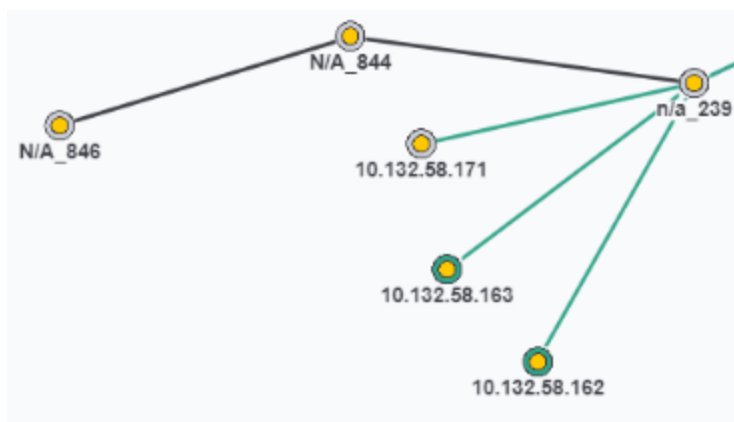


## Promoting unmanaged to 'look' managed and remove auto-inserted

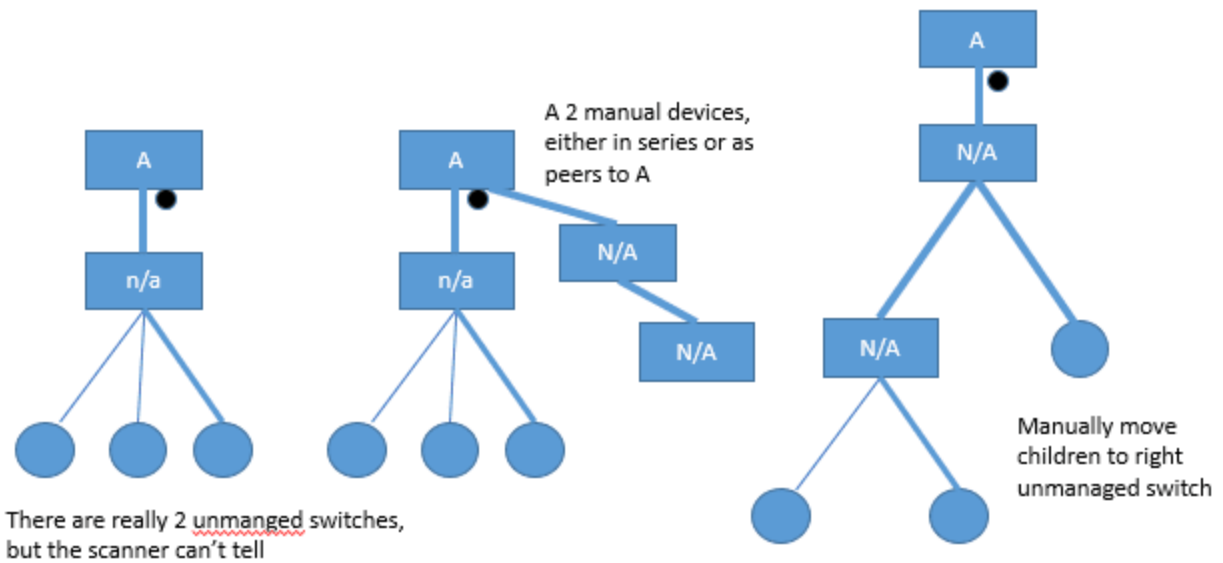


Search for "Device Configuration" and check the option "Virtual Machine, Unmanaged Switch" to device 'X' become the parent of the children in Map View that would replace that 'n/a' node.

### Manually Inserted Nodes



## Manually inserted nodes



### Upper case N/A nodes characteristics

Manually added by the user

May represent an unmanaged switch

Can show media conversion (copper to fiber and then fiber to copper)

Can show non-IP

# Supported Protocols

## EtherNet/IP: TCP/IP and Modbus/TCP

Intravue is only useful when all target devices support TCP/IP on IP V4, and particularly where the intervening devices such as routers and switches support SNMP.

The two primary industrial automation protocols which satisfy this requirement are Modbus/TCP and Ethernet/IP.

SNMP information and provide full topology (specially as devices in these networks are connected in a daisy-chain manner).

## PROFINET

**Profinet**<sup>1</sup> devices will also get discovered, monitored, and IntraVUE™ will be able to provide topology information through the use of the **LLDP**<sup>2</sup> protocol.

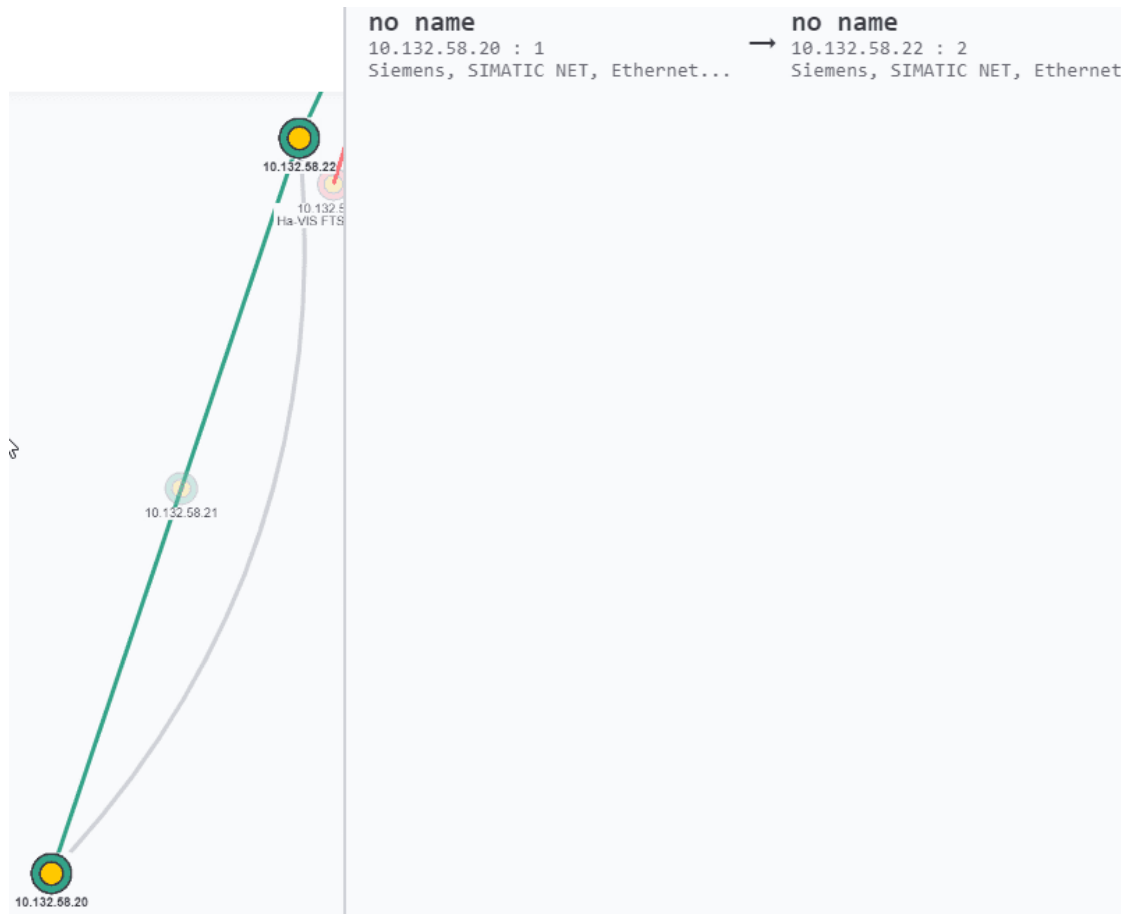
## LLDP Loop Detection

A misconfiguration in your network, equipment, or cabling may result in a loop. When this happens IntraVUE™ will draw a line between the two devices having the loop as curved gray line. If you click on that gray line it will show where are packets being sent from and to. The loop will continue remain active until something causes a device in the "loop" to move (i.e. depending on which device(s) move, the loop will disappear accordingly).

---

<sup>1</sup>is an industry technical standard for data communication over Industrial Ethernet, designed for collecting data from, and controlling, equipment in industrial systems, with a particular strength in delivering data under tight time constraints (on the order of 1ms or less).

<sup>2</sup>The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP is formalized in the IEEE 802.1AB standard. LLDP does advertise the hostname, management IP Address, port name an description.



LLDP is enabled by default. There will be times where you would want to disable LLDP to prevent it from moving. You can disable LLDP on a device by enabling the Edit Mode option "Disable All SNMP Requests" for that device. See [Device Configure - SNMP](#)

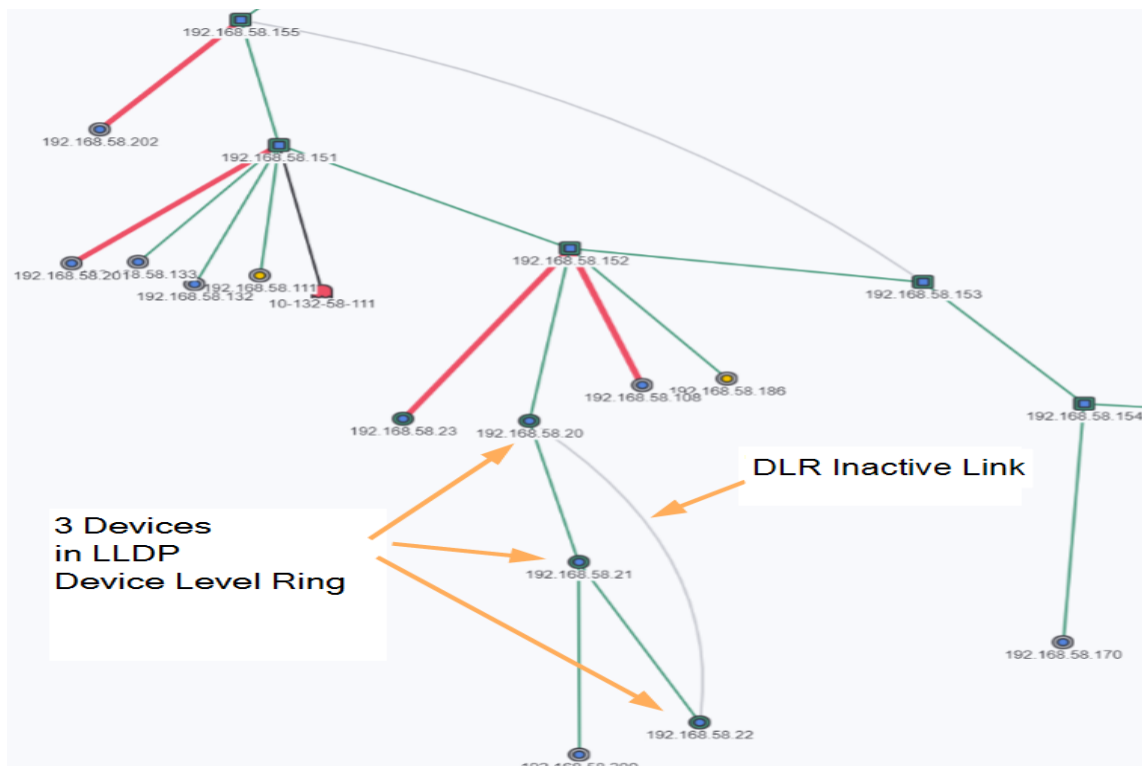
## Not Supported

The only exclusive 'Ethernet' only IA protocols such as EtherCat, Powerlink, Sercos, all use characteristics of their networks which IntraVUE™ is not set to measure, and so trying to use IntraVUE for fault diagnosis, discovery, and documentation is harder to do.

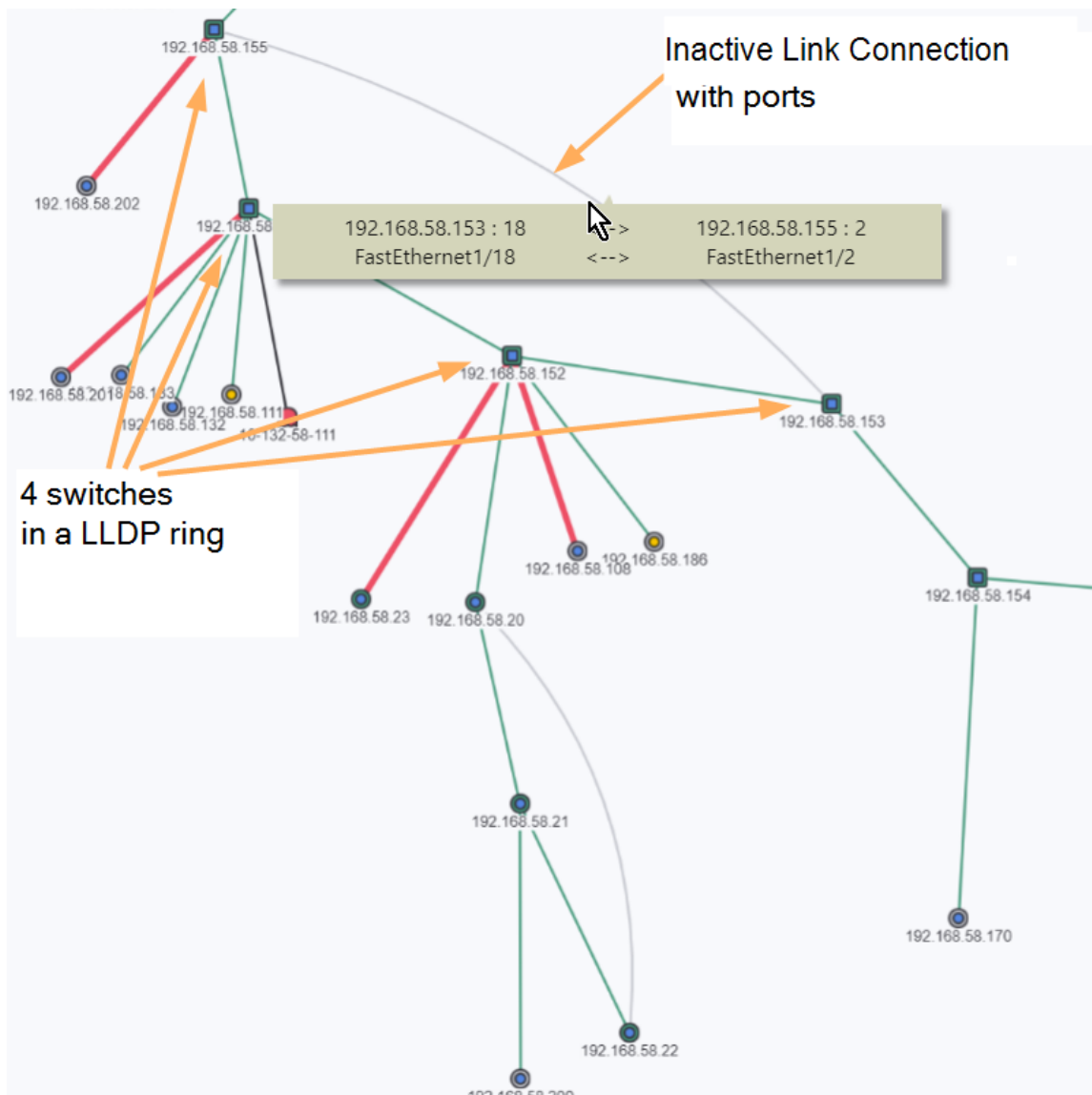
## Device (DLR) and Switch Level Ring Networks

When an LLDP device or a switch with SNMP enabled is setup in a device level ring or switch level ring network which is being detected by IntraVUE™ it will be graphed using the LLDP protocol with a trailing loop half-round circle shape going from the last device to the first device following the physical arrangement of the physical ring.

### Device Level Ring



### Switch Level Ring



By default, Switch to Switch LLDP connections are not made. This can be enabled in the `ivserver.properties` by setting the `lldp.switchToSwitch` property to 1. Enabling this option will increase the SNMP traffic.

The ring master will be the one to decide how to reorder devices when the ring breaks, or it may leave the ring in the current state until it breaks again.

IntraVUE simply shows the inactive link from the last device to the first device on the ring as a gray, curved line.

See also [Device Discovery & Management](#)



## IntraVUE Agent - Low Cost Agent

For control engineers that want to have visibility of their plant networks without sacrificing available budget, IntraVUE Agent software can be installed in a raspberry pi 3 unit that will allow the IntraVUE™ this to work as a regular agent but at a lower cost.

See this [link](#) for more information



## Deploying an IntraVUE™ Agent

The basic requirements to make use of the IntraVUE Agent are:

- Agent Readiness Checklist. See [Installation & Registration](#)
- Agent Deployment and placement. See [Using the IntraVUE Appliance as an Agent](#)
- Agent Configuration. See [IntraVUE Appliance Configuration](#)
- Good and stable bandwidth
- Local network access to the automation network (i.e. automation devices can be pinged from this agent).
- Access to the following ports through firewalls:
  - 65402 – used for communication to IntraVUE Agents
  - 65403 – used for communication to IntraVUE Agents
  - 8765 – mandatory port to browse IntraVUE

### **Additional Requirements for Virtual IntraVUE™ Agents**

The IntraVUE Agent also can also be installed in a virtual machine (linux). These are the requirements:

- A hypervisor (V-Spher, ESXi, or compatible)
- 2 GB ram OS Ram (4GB recommended)
- 64 GB disk space
- Single CPU
- Load the IntraVUE™ agent's image onto a virtual machine using the instructions here <http://i-vue.com/vmappliance/>

## Windows ARP Bursts

### Problem:

There have been a few recent reports of devices being adversely affected in combination with IntraVUE being used at the time of the incidents. This is limited to the scenario where the IntraVUE host is configured as the top parent, and there are sensitive devices in the local network.

### Cause:

We have determined that there is no issue with the IntraVUE software itself, but rather with the operating system on which IntraVUE is installed. We discovered that Microsoft made some changes to the way ARP packets are handled by the Windows' OS starting with Windows 7. This impacts any software that cause ARPs such as ping scanners, network monitors, and PCs \ VMs.

Before Windows 7 if an initial ARP was not answered in .5 seconds a first retry ARP was issued. If that ARP was not answered in another .5 seconds a second retry ARP was issued. These retries maintained the original timing of ARPs on the network.

Starting with Windows 7 at .5 second intervals all 'retry' ARPs that have not been answered are reissued in a burst. The spacing in the bursts is about 40 microseconds apart (wire speed) and does not conform to the Speed settings of IntraVUE.

Certain old devices within industrial networks cannot handle many ARP requests in a short time frame, which may cause them to reset. Examples of devices that can be affected include old PLCs (e.g. PLC5) and some I/O devices (e.g. bridges & gateways that communicate with old PLCs).

### Resolution:

In version 3.1 of the software we have implemented a temporary fix which slows the discovery and mitigates the problem. In order to revert the fix and return to the standard speeds, first confirm that one of the following is true for your network:

- 1) The host computer IP address is outside of the network with susceptible devices and use a Layer 3 switch \ router as the top parent for the network so ARP packets go through the Layer 3
- 2) An IntraVUE appliance is used as an Agent between the host computer and the network
- 3) An IntraVUE Appliance (Linux VM) or Microsoft Windows XP operating system is used as the IntraVUE host

After confirming the above modify the following line in the ...intravue\autoip\ivserver.properties file by putting a '#' symbol at the start of the following line at the bottom of the file.

```
unknown.devices.quota.max=2
```

Any customer having issues is encouraged to contact IntraVUE Tech Support (tech-support@panduit.com) for assistance in optimizing their system.

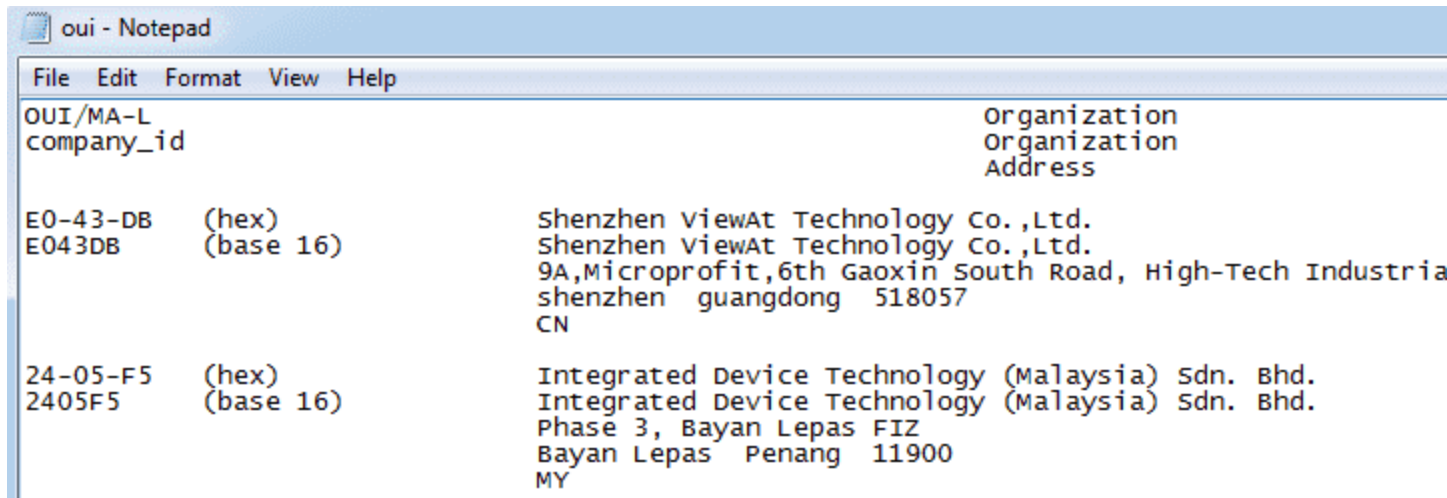
We are working with Microsoft to address this issue within their operating system and expect they should also be addressing this issue.

## Vendor Name from OUI

If a device supports Ethernet/IP or Profinet IntraVUE™ will automatically report the vendor name field, however, even when this is true there are times when a device will not have a vendor name reported. In that case IntraVUE™ will use the first three octets of such device's MAC address to do an OUI cross match look up against the IEEE oui.txt file included in the IntraVUE™ tomcat files and assign the missing vendor name for that device. The oui.txt file is located under C:\in-travue\autoip\tomcat8\webapps\scanext\WEB-INF\classes\

Basically the oui.txt file has the company ID (first three octets), Organization, and Address.

Whenever a vendor name is not reported or unknown to the IEEE Registration Authority the vendor name will appear as "IEEE Registration Authority". You will need to go into the oui.txt file and modify the organization's name and/or address to match you custom company information.



OUI/MA-L company_id		Organization Organization Address
E0-43-DB E043DB	(hex) (base 16)	Shenzhen viewAt Technology Co.,Ltd. Shenzhen ViewAt Technology Co.,Ltd. 9A,Micropofit,6th Gaoxin South Road, High-Tech Industria shenzhen guangdong 518057 CN
24-05-F5 2405F5	(hex) (base 16)	Integrated Device Technology (Malaysia) Sdn. Bhd. Integrated Device Technology (Malaysia) Sdn. Bhd. Phase 3, Bayan Lepas FIZ Bayan Lepas Penang 11900 MY

## Device Discovery & Management

### Ethernet/IP and PROFINET

IntraVUE can provide added value for installers and electricians when deploying new Industrial Devices to a network. By providing a live animated graphical view, one can easily confirm the location and status of devices being added. This verification confirms if the device's IP address is correctly configured and if it is actively communicating. However on larger networks in which multiple devices are being added, it may be difficult to know which IP is the correct device.

IntraVUE provides additional information by using the EtherNet/IP CIP, or the PROFINET protocol to obtain the vendor, model number, and version level of these newly added devices.

These additional details provide the installers with verification to reduce potential mistakes and simplify deployments. IntraVUE also automatically detects if the device has a web link and provides easy access to obtain additional details contained in these webpages.

Diagnostics



10.1.1.184  
FL IL 24 BK-ETH/IP-PAC

 **FL IL 24 BK-ETH/IP-PAC**  
10.1.1.184

EDIT

ADMIN VERIFY

**Device Info**

Default Details

Advanced Details

IP Address: 10.1.1.184

MAC Address: 00 A0 45 54 8B 8D

Critical Status: Always On

Admin Verified: No

Description: PLC to control

Owner: Electrical

Vendor: Phoenix Contact Electronics

Model: FL IL 24 BK-ETH/IP-PAC

Floor Layout: </Manuals/LocationLayout.pdf>

Web Link: <http://10.1.1.184/>

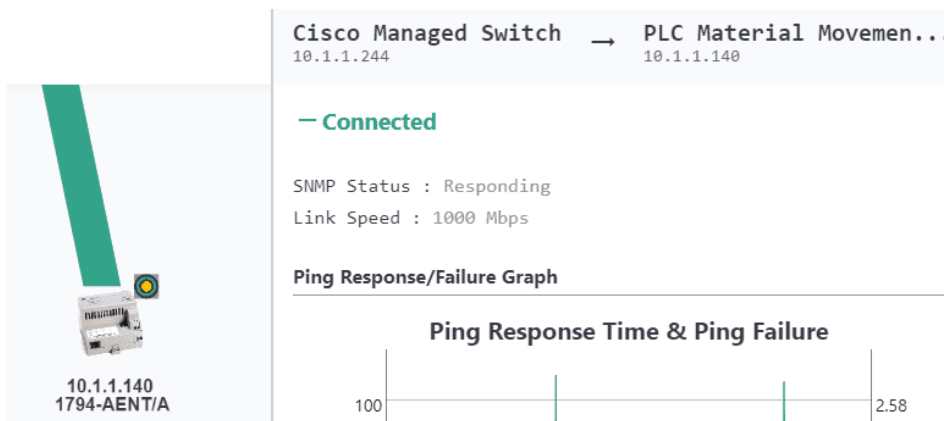
Maint. Log: </Manuals/MaintenanceLog.pdf>

Additional capabilities provide a graphical image associated with the model to provide even greater value to those responsible for adding these new devices, who may not be network experts such as technicians and electricians.

The connection side view will provide details on the IP address of the device (10.1.1.140) and the connected switch with the IP and port number (10.1.1.90:5).

Green connection lines indicate health communications while yellow or red indicate problems. Yellow indicating a specific parameter being exceeded and Red indicating a loss of communication. Additional verification can be accomplished by disconnecting the device and seeing the line go red. See also [Device \(DLR\) and Switch Level Ring Networks](#)

### Adding additional details to discovered devices



IntraVUE provides a means to add additional information and links to simplify support of these devices.

If the device supports SNMP the Device name and location will be automatically filled in with the SNMP data for these fields.

If the devices does not support SNMP, the information can be manually configured. Each device properties window allows for 12 links to obtain details about the device.

The devices web link is automatically populated but other links can be configured.

They can link specific data from a SCADA package or static information contained in PDF Documents.

These could include Maintenance Log, User Manual, Wiring Diagram, or installation details.

### **Device Management**

With many different devices being connected over time, it can be challenging to keep track of all the devices, their locations, and the version level. Using paper reports that have been prepared at an earlier time may not accurately represent the current network as devices can be added, replaced, or moved making static documents obsolete very quickly.

IntraVUE provides an accurate and dynamic means of managing all of the connected devices on your network. Networks with hundreds of devices are now easily managed by two methods.

1. Dynamic View with flexible search
2. On demand Spreadsheet Document

### **Dynamic View with flexible search**

Opening up the live animated view provides an easy method to view the current condition of any network. IntraVUE Search allows the searching for any partial text that is contained in the data fields. Data can be stored from automatically retrieved information such as the vendor, model, or Device name. Additionally the data could have been manually added such as a process description or functional area. Placing any part of the name will allow the search to locate all the devices that contain this detail in any field.

IntraVUE Search will provide details on how many devices match the search criteria with the first device centered on the screen and containing a purple indicator.

Topology

Plant Layout

851a

Device List

Filters

Event Log

Diagnostics

\*

X

View Details

IP Address	Device Name	MAC Add
10.1.1.71	MARK-PC	60 EB
10.1.1.171	Dell Managed Switch	00 11
10.1.1.137	Ethernet Direct Managed Switch	00 18
10.1.1.49	Printer	00 1B
10.1.1.95	CDOYLE-HP	88 51
10.1.1.83	CLAIRE-DESKTOP	00 11
10.1.1.188	N-TRON Managed Switch	00 07
10.1.1.63	Dell Managed Switch	78 2B
10.1.1.88	SUZANNE-PC	00 1A
10.1.1.57	Dell Wireless Router	00 C0
10.1.1.72	OP-JSAH-MACBOOK	28 5A

If there are more than one device found, you will see how many devices have been found. You can scroll through each.

Details on each will be filled in and when you select a device it will be centered on the screen. In this way you will not only be able to search for a specific device but also see the position of the device in the network. The Search function provides an easy method to select a specific detail such as a Device Name, Network Name, partial MAC, or IP address, or manually added data and view all of these found in your network.



## SMS Notifications

IntraVUE can send SMS notifications to phones that already have SMS notifications configured whenever they receive an email. This forwarding mechanism allows the phone carrier or third-party to forward every email or specific emails to be sent to a cellular phone in SMS format. We recommend contacting your cellular carrier or email provider on how to enable email forwarding to SMS for your cell phone.

## View Databases Offline

Viewing IntraVUE databases in offline mode helps you see a virtual "live snapshot" of how your network performance at one point in time without having the IntraVUE scanner running. This is helpful for when you want to backtrack to an earlier date before an incident or change occurred, to provide analytics to an integrator or support personnel for review, or simply load to a newer machine.

1. Open a browser and go to <http://127.0.0.1:8765>
2. In the IntraVUE™ Browser, Click Configure (Login as Admin)
3. Select the Database tab
4. Click "Restore"
5. Check the box "KEEP INTRAVUE SCANNER OFFLINE AFTER DATABASE RESTORE"
6. Select "Off-line\_Demo\_Database.dmp" from the list and click "Restore Database"
7. Wait for a "Success" message
8. Click "View" from the navigation menu and you're all done

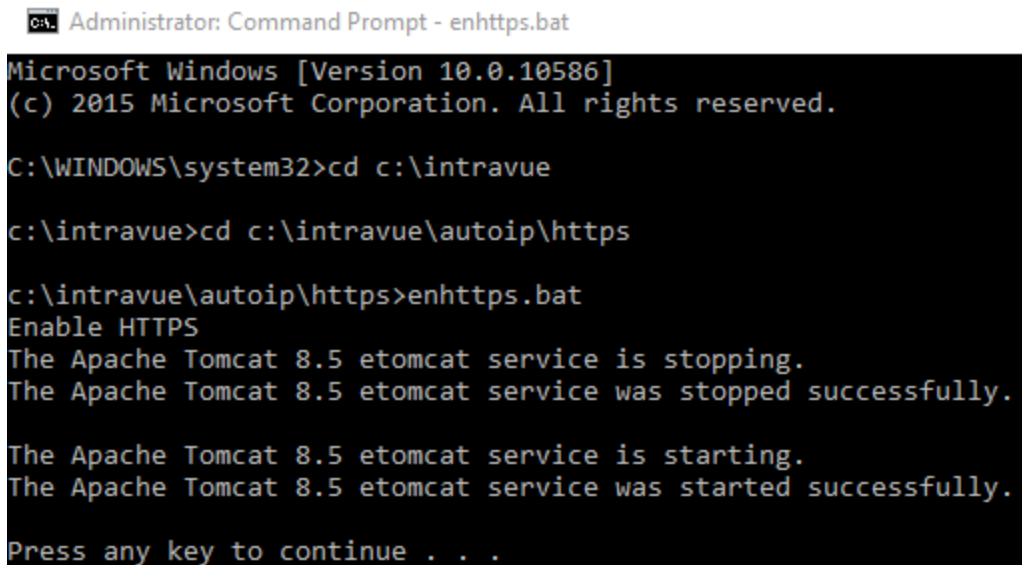
## HTTPS

Many publications including NIST, ANSI, CCSC, and others concerned about industrial controls security recommend that any remotely accessible web servers make use of HTTPS rather than HTTP because of cyber risks. IntraVUE™ can be configured to use an included self-signed certificate, or a certificate from a trusted certificate authority (CA). This feature is available on IntraVUE™ 3.1 or later. Contact [techsupport@panduit.com](mailto:techsupport@panduit.com) to request a copy of the document that walks you through implementing HTTPS.

### Windows Instructions

To enable HTTPS follow these steps:

1. Go to windows start > type 'CMD' > right-click "Command Prompt" > select "Run As Administrator"
2. Type **cd c:\intravue\autoip\https\**
3. Type **enhttps.bat**
4. The "Apache Tomcat 8.5 eTomcat" service will be restarted
5. Open a new browser window and point your browser to **https://127.0.0.1:8766**




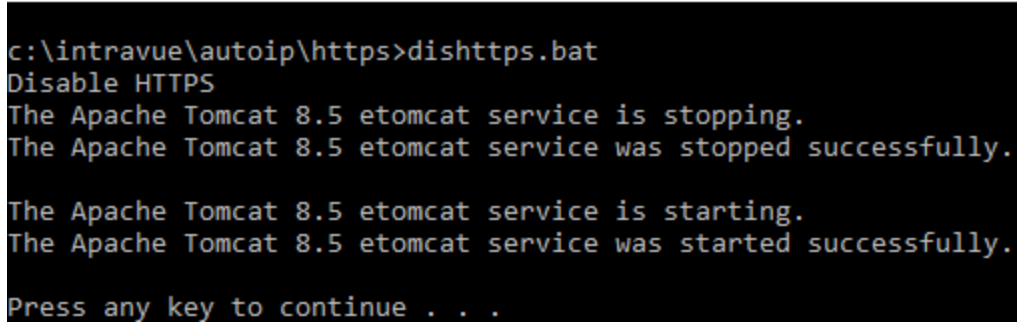
```
C:\WINDOWS\system32>cd c:\intravue
c:\intravue>cd c:\intravue\autoip\https
c:\intravue\autoip\https>enhttps.bat
Enable HTTPS
The Apache Tomcat 8.5 etomcat service is stopping.
The Apache Tomcat 8.5 etomcat service was stopped successfully.

The Apache Tomcat 8.5 etomcat service is starting.
The Apache Tomcat 8.5 etomcat service was started successfully.
Press any key to continue . . .
```

To disable HTTPS follow these steps:

1. Go to windows start > type 'CMD' > right-click "Command Prompt" > select "Run As Administrator"
2. Type **cd c:\intravue\autoip\https\**
3. Type **dishttps.bat**
4. The "Apache Tomcat 8.5 eTomcat" service will be restarted
5. Open a new browser window and point your browser to **http://127.0.0.1:8765**

 Administrator: Command Prompt - dishttps.bat



```
c:\intravue\autoip\https>dishttps.bat
Disable HTTPS
The Apache Tomcat 8.5 etomcat service is stopping.
The Apache Tomcat 8.5 etomcat service was stopped successfully.

The Apache Tomcat 8.5 etomcat service is starting.
The Apache Tomcat 8.5 etomcat service was started successfully.

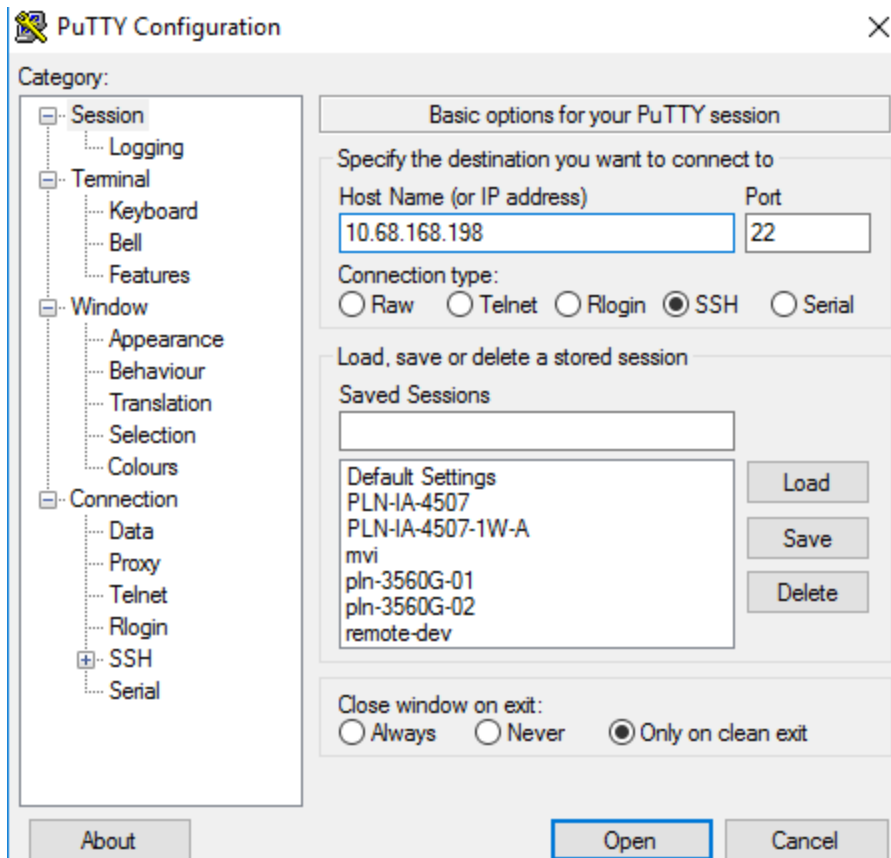
Press any key to continue . . .
```

Both https.config and dishttps.bat are located under C:\intravue\autoip\https\

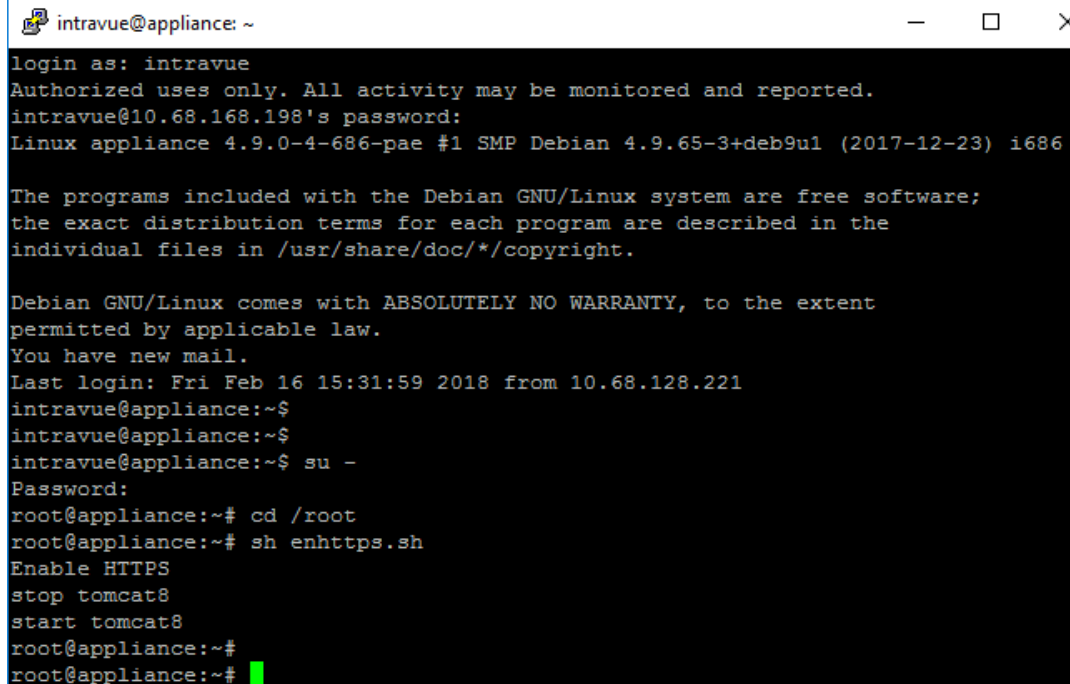
## IntraVUE Appliance Instructions

To enable HTTPS for an appliance follow these steps:

1. Putty into the IntraVUE™ Appliance by using SSH and the IP address of the IntraVUE appliance



1. Log in with username 'intravue' and password 'intravue'
2. Elevate to root privileges using by typing command 'su -' and using the root password
3. Change directory to home of root by typing 'cd /root'
4. Type **sh enhttps.sh** and hit 'Enter'
5. The "Apache Tomcat 8.5 eTomcat" service will be restarted
6. Open a new browser window and point your browser to **https://127.0.0.1:8766**



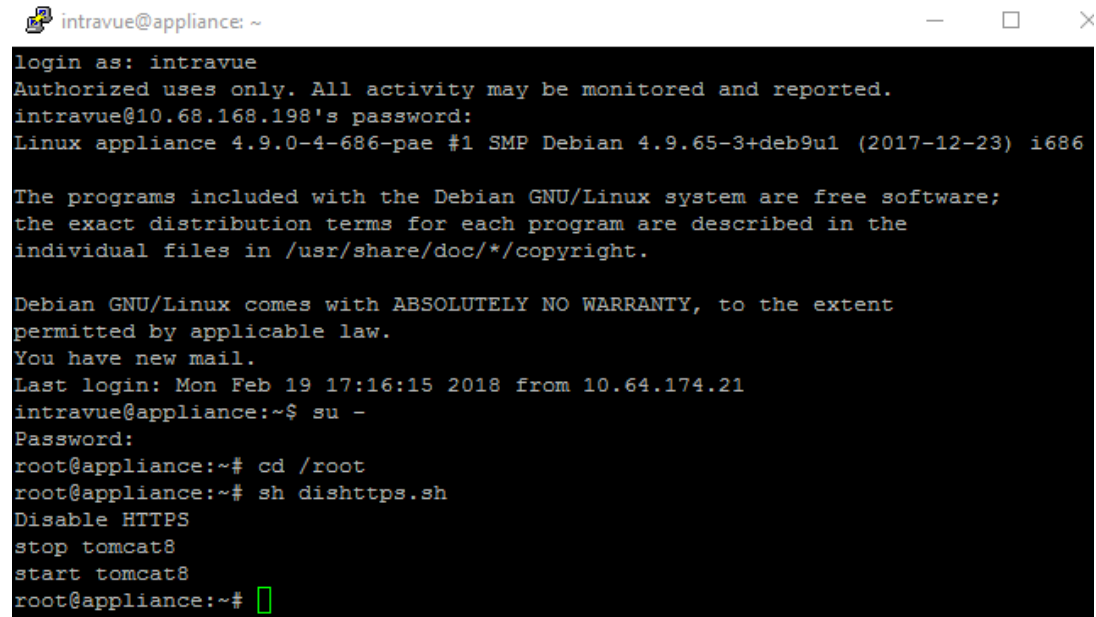
```
intravue@appliance: ~
login as: intravue
Authorized uses only. All activity may be monitored and reported.
intravue@10.68.168.198's password:
Linux appliance 4.9.0-4-686-pae #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Feb 16 15:31:59 2018 from 10.68.128.221
intravue@appliance:~$
intravue@appliance:~$
intravue@appliance:~$ su -
Password:
root@appliance:~# cd /root
root@appliance:~# sh enhttps.sh
Enable HTTPS
stop tomcat8
start tomcat8
root@appliance:~#
root@appliance:~#
```

To disable HTTPS for an appliance follow these steps:

1. Putty into the IntraVUE™ Appliance using SSH and the IP address of the IntraVUE appliance
2. Log in with username 'intravue' password 'intravue'
3. Elevate to root privileges using by typing command 'su -' and using the root password
4. Change directory to home of root by typing 'cd /root'
5. Type **sh dishttps.sh** and hit 'Enter'
6. The "Apache Tomcat 8.5 eTomcat" service will be restarted
7. Open a new browser window and point your browser to **http://127.0.0.1:8765**



```
intravue@appliance: ~  
login as: intravue  
Authorized uses only. All activity may be monitored and reported.  
intravue@10.68.168.198's password:  
Linux appliance 4.9.0-4-686-pae #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
Last login: Mon Feb 19 17:16:15 2018 from 10.64.174.21  
intravue@appliance:~$ su -  
Password:  
root@appliance:~# cd /root  
root@appliance:~# sh dishttps.sh  
Disable HTTPS  
stop tomcat8  
start tomcat8  
root@appliance:~#
```

## Using HTTPS

HTTPS requires a certificate to validate the site the user is connected to is what site they want. The certificate contains the domain name of the site.

IntraVUE is shipped with a self-signed certificate that allows all traffic on the wire to be encrypted but will not be treated as 'secure' by most browsers because the domain of the computer IntraVUE is installed on is not in the certificate supplied by default.

By default, when HTTPS is enabled, a self-signed certificate is applied. When using an IP address within the browser you will see the following, but the traffic on the wire will be encrypted:



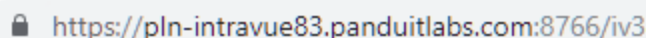
By default, when HTTPS is enabled a self-signed certificate is applied. When using a fully qualified domain name within the browser you will see the following, but the traffic on the wire will be encrypted:



If a user has their own certificate, they can follow these instructions to replace the default certificate on their own.

- » Create a Keystore called https.keystore in \intravue\autoip\https folder which contains the CA certificate. Follow instructions on how to import a certificate into a keystore from tomcat web-site. [https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html#Installing\\_a\\_Certificate\\_from\\_a\\_Certificate\\_Authority](https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html#Installing_a_Certificate_from_a_Certificate_Authority)
- » Enter the password for the keystore in https.config file in \intravue\autoip\https folder
- » Enable HTTPS following the steps listed in the above section.

If a certificate from a trusted certificate authority (CA) is applied, the user should see the following when using the domain name for browsing:





If a certificate from a trusted certificate authority (CA) is applied and an IP address is used to browse instead of the domain name where the cert was assigned then the user will see the following, but the traffic on the wire will be encrypted:

A screenshot of a browser's address bar. On the left, there is a red warning icon (a triangle with an exclamation mark) followed by the text "Not secure" in red. To the right of this, separated by a vertical line, is the URL "https://10.132.56.83:8766/iv3," where the "https://" part is in red and the rest of the URL is in blue. The entire address bar has a light gray background.

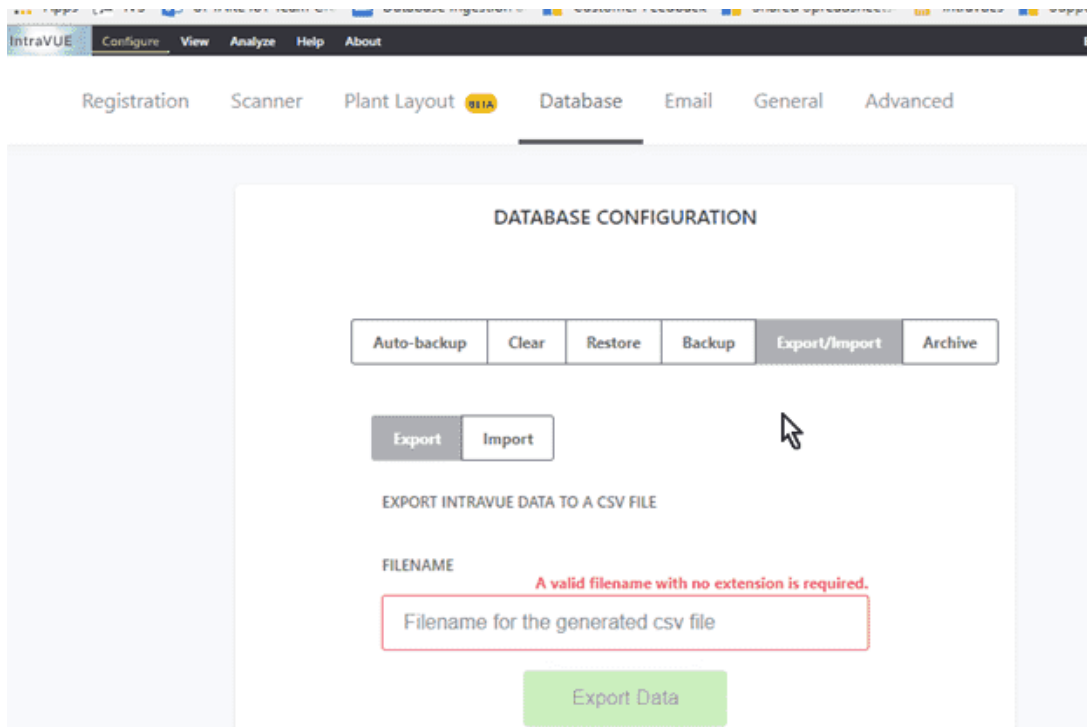
⚠ Not secure | https://10.132.56.83:8766/iv3,

## Importing Device Names From Third Party Sources

These steps explain how to merge a list of IP Addresses and Names and into a CSV file exported from IntraVUE.

The process uses the Excel Macro VLOOKUP to change the names exported from IntraVUE to the names in your list.

Step 1 – Use the IntraVUE export function and save a CSV file.

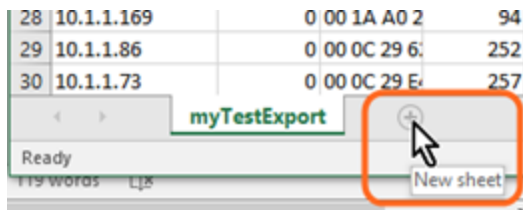


Step 2 – Open the saved file in Excel

The image below shows the IP and DeviceViewName columns expanded.

	A	B	C	D	E	F	G	H	I	J	K	L
1	IP	Active	MAC	Ref	ParentRef	ParentIP	ParentPor	UplinkPor	DeviceViewName	DeviceVie	DeviceVie	Device
2	10.1.1.71		1 60 EB 69 D	5	1		0	0	MARK-PC	Floor Layc	/Manuals	
3	10.1.1.171		1 00 11 43 84	90	5	10.1.1.71	0	19	Dell Managed Switch	Floor Layc	/Manuals	
4	10.1.1.137		1 00 18 A9 0	132	90	10.1.1.171	5	8	Ethernet Direct Managed Switch	Floor Layc	/Manuals	
5	10.1.1.49		1 00 1B A9 8	22	132	10.1.1.137	1	0	Printer	Floor Layc	/Manuals	
6	10.1.1.95		1 88 51 FB 5	50	132	10.1.1.137	5	0	CDOYLE-HP	Floor Layc	/Manuals	
7	10.1.1.83		1 00 11 11 B	64	132	10.1.1.137	6	0	CLAIRE-DESKTOP	Floor Layc	/Manuals	
8	10.1.1.188		1 00 07 AF F	108	90	10.1.1.171	13	1	N-TRON Managed Switch	Floor Layc	/Manuals	
9	10.1.1.63		1 78 2B CB E	275	108	10.1.1.188	2	0	Dell Managed Switch	Floor Layc	/Manuals	
10	10.1.1.88		1 00 1A A0 2	54	108	10.1.1.188	3	0	SUZANNE-PC	Floor Layc	/Manuals	
11	10.1.1.57		1 00 C0 A8 E	98	108	10.1.1.188	7	0	Dell Wireless Router	Floor Layc	/Manuals	
12	10.1.1.72		0 28 5A EB 4	30	98	10.1.1.57	0	0	OP-JSAH-MACBOOK	Floor Layc	/Manuals	
13	10.1.1.76		1 8C 58 77 9	150	98	10.1.1.57	0	0	BILL-MACBOOK	Floor Layc	/Manuals	

Step 3 – Add a new sheet to Excel



Step 4 – Use copy/paste to select the IP Addresses and Names you want to import from another document (Excel, Word, text) and save them in the new sheet, Sheet1 in this example. You do not need to have a header row.

Step 5 – In the main sheet, myTestExport in this example, copy the DeviceViewName column, then right click on the DeviceViewName column and 'insert copied cells'. A new column J should appear with the same name. There should now be two columns with the same name and contents, I and J.

Step 6 – Enter the macro below into the NEW top DeviceViewName cell, J2. Note: the macro's column and row numbers are specific to the first row of data under DeviceViewName column.

`=IFNA(IF(I2="no name",VLOOKUP($A2,Sheet1!$A$1:$B$4085,2,FALSE),I2),"no name")`

NOTE: The \$A2 above refers to the first row having an IP in the main sheet, Sheet1\$A\$1 is the first row in the column of Shee1 that has an IP address and the \$B\$4085 is the end of the block having both IP and names. It can contain empty rows, as in this case.

Step 7 – Copy cell J2 and paste it into all the remaining cells of column J

Step 8 – Copy Column J and then right click on Column I > Paste Special > Values. Use Values because we don't want to copy the formulas from Column J.

As a result, any cell in column I that had 'no name' and which has data for that IP in sheet 1 will have the name from sheet1 in column J.

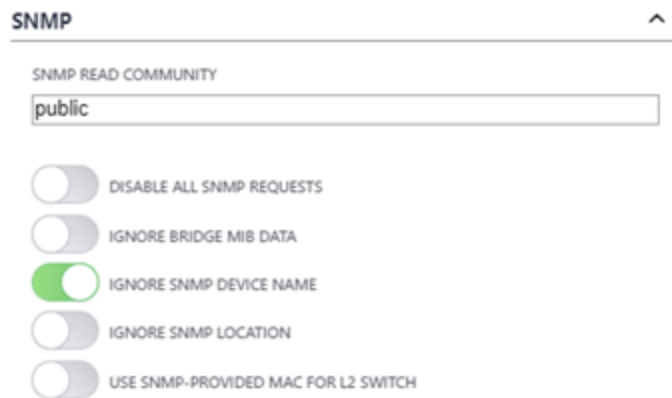
Step 9 – Delete column J, leaving only one column labeled DeviceViewName. (Column J had formulas, not names)

Step 10 – Save as CSV and import into IntraVUE.

Other Notes

This macro is written so that existing names in column I are NOT overwritten. The macro can be modified if you want to overwrite all names based on the data in Sheet1.

If you overwrite the names found by IntraVUE they will be overwritten in a future scan cycle if the 'ignore snmp device name' is not enabled.



If you overwrite the names found by IntraVUE they will be overwritten in a future scan cycle if the 'ignore snmp device name' is not enabled.

You can do this in the CSV file by setting a value in the snmp.suppress column. The values are explained at <http://www.i-vue.com/iv3/help/IntravueHelp.htm#CSVColumnValuesIv3.htm>

SNMP.supress 1 - Disable all SNMP requests,

2 - Ignore SNMP Bridge Mib data.

4 - Ignore SNMP Location,

8 - Ignore SNMP Device Name,

You can add up all or multiple values and enter that value (e.g. 12 = 8 + 4).

## Solutions

## Can't view IntraVUE remotely

### Problem:

Can't see IntraVUE™ from remotely from my laptop

### Solution:

Check a few things before assuming there's an issue with the IntraVUE™ host.

1. Ping the IntraVUE™ host and make sure you get a good ping response
2. From the IntraVUE™ host open URL `http://127.0.0.1:8765` in your browser and verify you see a topology.
3. From the IntraVUE™ host open URL `http://x.x.x.x:8765` (where x.x.x.x is the IP address of the host on the network) in your browser and verify you see a topology.
4. Check / Change Windows firewall settings on the IntraVUE™ host.
  - » Go to start, search "firewall" > select Windows Firewall with Advanced Security
  - » Right-click Inbound Rules > New Rule
  - » Select Port > In specific local ports type "8765", Next
  - » Select "Allow the connection", Next
  - » Hit Next for ALL (domain, private, public) checked
  - » Type a name and description and hit "finish"

## White screen after upgrade

### Problem:

After performing an upgrade to Intravue 3.1 and clicking on browse intravue nothing appears on the screen except that the browser opens with a blank screen.

### Solution:

To resolve this issue check the following

1. Make sure that the AutoIP I-Server, AutoIPPingDaemon, and Mysql services are running.  
Go to start > search for 'services'. If any of these services are down, try to start them by doing a right-click > start.
2. If the services can not be started or you get an error saying "Windows could not start the mysql service on local computer. Error 1067: The process terminated unexpectedly", then most likely this is a lethal error and you would have to perform the next steps to fix this behavior.
3. Stop all intravue services including AutoIP I-Server, AutoIPPingDaemon, AutoIP Auto Bootp, Apache Tomcat, and Mysql
4. Go to start > run (or search windows in windows 10) > type 'cmd' and right-click on the application "command prompt" and select "Run as administrator". Accept the warning and click 'Yes'.
5. Delete each intravue service by typing "sc delete [nameOfService]" where "nameOfService" is mentioned below for each service:
  1. 'etomcat'
  2. 'AutoIP Auto Bootp'
  3. 'AutoIP I-Server'
  4. 'AutoIPPingDaemon'
  5. 'mysql'
6. Go to C:\ and rename the 'intravue' folder to something different (e.g. intravueOld)

7. Right-click the intravue installer and select 'Run as admin'
8. Complete the installation and verify that intravue topology comes up fine when the browser opens.



## Mysql service not being installed by the intravue installer

### Problem:

After performing an upgrade intravue 3.1 user interface opens but doesn't show the topology. The mysql service is not installed

### Solution:

To resolve this issue check the following

1. Check log information in C:\intravue\intravue\_install
2. Check C:\mysql\data and copy the \*.err. Read the copy with notepad
3. Make a back up of c:\intravue
4. Go to "Add & Remove Programs"
  1. Delete intravue
  2. Delete intravue extended service
  3. Delete java
  4. Delete mysql
  5. Delete auto ip
5. Delete the Intravue services using 'sc delete [servicename]'
6. Delete the c:\intravue folder
7. Delete c:\program files(x86)\java
8. Go c:\mysql\bin and delete the mysqld.exe.
9. Reboot the machine
10. Run the latest installer as 'administrator'
11. Make sure all of these services are running
  1. AutoIP-I-Server
  2. AutoIP Bootp
  3. AutoIP Ping Daemon

4. Apache eTomcat

5. MySQL

12. If the mysql service is not running there might be a chance that intravue key in the registry is pointing to a different drive (e.g. F:\intravue instead of C:\intravue)
13. If problem persists contact [techsupport@panduit.com](mailto:techsupport@panduit.com)

## Can Intravue scan Profibus networks?

### Question

Can Intravue scan profibus networks?

### Answer

No. See [Supported Protocols](#)

## How to print the Intravue topology from a plotter?

### **Problem:**

How to print the intravue topology from a plotter?

### **Solution:**

See Plant Layout in [Creating Plant Documentation](#)

## Cisco Switches with IPDT Cause Duplicate IPs

### Problem:

Allen-Bradley Ethernet module faulting with the following scrolling message:

Module #1:

1756-ENBT/A

[IP Address]

Message:

Duplicate IP

84b51768b631

PLC connected to a Cisco 3850

### Cause

IOS Bug on Cisco switches (e.g. IE300, C3850, C3650) See <https://bst.cloud-apps.cisco.com/bugsearch/bug/CSCuj04986>

### Solution:

Run these two commands to completely disable the ip device tracking function on the affected Cisco switches that have this IOS bug

**Hostname (config)#nmosp attach suppress**

**Hostname (config)#no ip device tracking max**

Or

follow the workarounds below depending on your firmware version

Full Cisco Article

568750 False Duplicate IP detection on Ethernet modules when used with Cisco switches

Problem

When Rockwell Automation EtherNet/IP modules are connected to a subnet containing Cisco switches with "IP device tracking" (IPDT) enabled, the modules may go into a duplicate IP address

state after a restart/reset.

#### Environment

Any layer two networks that contain both Rockwell Automation EtherNet/IP modules and Cisco switches running IPDT.

IPDT is much more likely to be implemented on Cisco switches as of August, 2013 because of a behavior change which enables this command if any feature which requires it is enabled.

This behavior change also removes the ability to turn off IPDT without first turning off any features which require IPDT. The Stratix line of switches will not have “IP device tracking” enabled by default until a permanent solution is in place.

#### Cause

The IPDT feature sends probe ARP packets with a source IP address of 0.0.0.0., the source MAC ID of the switch, and the target IP and MAC ID for the device being probed to check that it is still connected and responsive.

When a device becomes disconnected, and then is reconnected within the configurable IPDT timeout period, probe ARP packets may be received by a Logix Ethernet module at the same time as it is in its Address Conflict Detection mechanism. If this happens, the EtherNet/IP module will immediately go into a duplicate IP state, and stop communicating.

IPDT when activated on a Cisco switch will try to probe for every IP connected on the subnet, regardless of whether it is connected to that switch or not.

Testing has shown that this affects the majority of Ethernet modules sold by Rockwell Automation.

#### Solution

Cisco is continually updating the latest workarounds. Here is a link to Cisco’s technote: <http://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html>

#### Workaround

Several workarounds to this issue exist. They all make suggestions using Cisco IOS command line interface commands.

#### Workaround 1

Architect manufacturing zone subnets such that:

1. IPDT is explicitly disabled on every trunk port with the following command:

```
Hostname (config)# ip device tracking maximum 0
```

2. IPDT probe delay is manually configured on any access port connected to a Rockwell Automation Ethernet module with the following command:

```
Hostname (config)# ip device tracking probe delay 10
```

### Workaround 2

If the switch in question has an administration IP (SVI) configured on the subnet/VLAN in question the Cisco CLI command: `Hostname (config)# ip device tracking probe usesvi`

will insert the administration IP into the source IP in the IPDT packet. This packet will not impact Address Conflict Detection operation.

### Workaround 3

Disable IPDT on any Cisco switch ports with IPDT enabled that subsequently connect to a Rockwell Automation Ethernet module with the following command:

```
Hostname (config)# ip device tracking maximum 0
```

### Workaround 4

Run both the **tracking probe auto-source** command and the **tracking probe auto-source fallback** on all switches with this feature turned on.

See <https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html>

### Additional Links

IPDT Overview - <https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html>

Cisco Community Discussion - <https://supportforums.cisco.com/discussion/12563251/cisco-switch-upgrade-leads-allen-bradley-plc-duplicate-ip-address-errors>

Honeywell Community Discussion - <https://->

[dashboard.intelligrated.com/knowledgebase/PrintArticle.aspx?article=59affed0-03ec-4c12-a40c-2a14f43fc5d3](http://dashboard.intelligrated.com/knowledgebase/PrintArticle.aspx?article=59affed0-03ec-4c12-a40c-2a14f43fc5d3)



## Known Issues

Issue	Affected Version (s)	Solution / Work-around
Warning - display data is not current. License count exceeded because software registration is not valid"	2.x	Contact Support to register product first.
"Warning - display data is not current. Scanner does not appear to be running"	2.x	Make sure the AutoIP I-Server and Auto-IP Ping Daemon are running in windows services.
"Warning - display data is not current Scanner is in OFFLINE mode"	2.x	Make sure the AutoIP I-Server and AutoIP Ping Daemon are running in windows services.  OR  Database was loaded OFFLINE. This is for only for testing and troubleshooting.

		<p>To load your database back to live mode, log in as admin, open System Configuration, Database, Restore Database From File. Select 'Yes' to stop scanner and replace current database, and select the same database without selecting 'Restore Database OFFLINE' option. Click 'OK', 'OK' to success message, and 'Apply and Close'.</p>
<p>KPI status shows “This system does not have a valid service contract code”</p>	<p>2.x</p>	<p>Verify that in “Enter product registration” the service contract code is present and it's status is set to OK. Otherwise, contact</p>

		support to request a new service contract code.
The search feature does not move to the correct node on Internet Explorer	2.x	In the IE browser go to Tools, Compatibility View settings, and add the IP address of IntraVUE.
IntraVUE doesn't work with the Chrome browser	2.x	We haven't fully tested with Chrome. We recommend using IE 11 (or later) and Firefox 45 (or later).
<b>HSRP - HOT STANDBY REDUNDANT PROTOCOL</b>  <b>HSRP</b> allows two Layer 3 Switches (Routers) to be connected and share data. If one router fails, the other will assume all functions of the other. To complete the redundancy, the upper level Layer 2 switches are redundantly connected to each router. This has the potential for network traffic to take different paths at any time, although in practice it happens rarely.	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<b>CISCO 2950 Switches</b>  The port numbers on the switch faceplate are the reverse of this switches internal port numbers, the numbers used by IntraVUE. Port 1 is reported as 12, 2 as 11, etc.	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs

<p><b>HIRSCHMANN Switches</b></p> <p>Early versions of Hirschmann Mach switches did not report the Bridge Mib (RFC 1493) and instead used the Q-Mib. The Bridge Mib tells the port number for a MAC address, the Q-Mib is a newer standard designed to handle VLANs. The Q-Mib requires the Bridge Mib also be reported. The Bridge Mib is what IntraVUE uses to determine topology.</p> <p>Current versions of the Mach switches support the Bridge Mib. If you don't see devices being place by IntraVUE under a Mach switch, you probably need to update the firmware of the switch.</p> <p>Early models of some Hirschmann switches (4000, IP67) reported devices having mac addresses that were numerically close as if they were the same mac. For instance, two devices with mac addresses like 00 00 BC 32 F2 7F and 00 00 BC 32 F2 83 where the last octets are close, could be reported by one of these switches as being on a port when in fact it was not.</p>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<p><b>HEWLETT PACKARD PROCURVE 2810 Switches</b></p> <p>This switch had an issue responding to SNMP GetNext requests in certain conditions. Software version N.11.15 corrects this behavior.</p>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<p><b>HEWLETT PACKARD PROCURVE 1810G Switches</b></p>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<p><b>WEIDMUELLER IE-SW22/2F-M V4.9 Switches</b></p>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<p><b>GARRETCOM Switches</b></p>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs

<b>RUGGEDCOM Switches</b>	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs
<b>CISCO IE3000, C3600 Series, C3800 Series Switches</b> can cause duplicate IPs for devices connecting to them (e.g. PLCs).	Any	See <a href="#">FAQs</a> , Known Switch Issues FAQs

## FAQs

### GENERAL FAQs

[Q: WHY DOES A BLANK WINDOW OR NO WINDOW APPEAR WHEN I CLICK ON A MENU ITEM?](#)

[Q: WHY DOES A BLANK WINDOW APPEAR WHEN I BROWSE TO INTRAVUE?](#)

[Q: HOW DO I GET MORE INFORMATION WHEN THE 'TEST EMAIL' BUTTON DOESN'T WORK?](#)

[Q: HOW LONG DOES IT TAKE INTRAVUE DO FIND NEW DEVICES?](#)

[Q: WHAT ARE AUTO INSERTED NODES \(N/A IN IP VIEW\)?](#)

[Q: WHAT DOES THE RED MESSAGE 'DATA OUT OF DATE' MEAN?](#)

[Q: I HAVE A 16-PORT SWITCH. WHY DOES INTRAVUE SHOW PORT NUMBERS LIKE 35 OR 958?](#)

[Q: CAN NON-ETHERNET DEVICES BE DISPLAYED IN THE INTRAVUE SOFTWARE?](#)

[Q: WHY DOES ALL THE THRESHOLD DATA GO TO ZERO SOMETIMES?](#)

[Q: HOW CAN I SET ALL OR MANY DEVICES TO BE ENABLED FOR EMAIL ALARMS?](#)

[Q: WHY DO THRESHOLD VALUES GET SMALLER WHEN I LOOK AT OLDER DATA?](#)

[Q: HOW CAN I STOP AND START INTRAVUE SERVICES ON MY LAPTOP?](#)

[Q: DOES INTRAVUE USE AN EXPLICIT MESSAGE WITH CIP CONNECTION WHEN TALKING WITH A EtherNet/IP DEVICE?](#)

### INSTALLATION AND SYSTEM REQUIREMENTS FAQs

[Q: WHAT ARE THE RECOMMENDED SYSTEM REQUIREMENTS?](#)

[Q: HOW MUCH NETWORK TRAFFIC IS GENERATED BY INTRAVUE AND THE INTRAVUE SUPERVISOR?](#)

[Q: WHAT PORTS ARE USED BY INTRAVUE?](#)

## CONFIGURATION QUESTIONS

[Q: IS THERE AN EASY WAY TO ADMIN VERIFY ALL THE DEVICES?](#)

[Q: WHY ARE ALL OR MOST THE DEVICES UNDER AN UNRESOLVED NODE?](#)

[Q: I HAVE MANY INTRAVUE NETWORKS, CAN I ONLY SHOW ONE OR TWO AT A TIME?](#)

[Q: CAN INTRAVUE SCAN THROUGH A FIREWALL AND IF SO, HOW?](#)

[Q: CAN I BACKUP INTRAVUE FROM A DOS COMMAND PROMPT?](#)

[Q: HOW CAN I GET BETTER PORT NUMBERS FOR CISCO SWITCHES THAT ARE STACKED?](#)

[Q: HOW DO I CHANGE THE PASSWORD FOR INTRAVUE?](#)

## DIAGNOSING NETWORK ISSUES

[Q: WHAT IS CONSIDERED A PING FAILURE?](#)

[Q: WHAT IS NORMAL VS DISCONNECT?](#)

[Q: HOW DO I DIAGNOSE PING FAILURES?](#)

[Q: HOW ARE DUPLICATE MAC ADDRESSES DISPLAYED?](#)

[Q: HOW ARE DUPLICATE IP ADDRESSES DISPLAYED?](#)

[Q: I CAN PING A DEVICE FROM DOS, WHY DOESN'T INTRAVUE DISCOVER IT?](#)

[Q: CAN INTRAVUE SCAN MESH NETWORKS?](#)

## MySQL

[Q: THE MYSQL FOLDER HAS GIGABYTES OF DATA, HOW TO I MAKE IT SMALLER?](#)

[Q: CAN I EXPORT EVENTS FROM THE EVENT LOG?](#)

[Q: IT IS POSSIBLE TO COMBINE THE SQL FILE AND THE DOS COMMAND INTO A SINGLE BATCH FILE AS SHOWN IN THE FOLLOWING EXAMPLE?](#)

## **IntraVUE™ AND SYNAPSENSE**

[Q: CAN INTRAVUE AND SYNAPSE WORK ON THE SAME MACHINE?](#)

## **Modbus/TCP**

[Q: IS THERE A TOOL AVAILABLE TO HELP DEBUG MODBUS ISSUES?](#)

## **PLUG AND APPLIANCES FAQs**

[Q: HOW DO YOU REPLACE THE MICRO SD MEMORY CARD?](#)

[Q: HOW DO YOU CHANGE/SET THE DATE, TIME, AND/OR TIME ZONE ON THE PLUG?](#)

## **INTRAVUE & JAVA FAQs**

[Q: WHAT MUST BE CONFIGURED BEFORE JAVA WILL WORK WITH INTRAVUE IN MY BROWSER?](#)

[Q: WHY DOESN'T SEARCH CENTERS A DEVICE IN INTERNET EXPLORER 11?](#)

[Q: INTRAVUE IN THE BROWSER IS TAKING A LONG TIME TO LOAD, WHY?](#)

## **INTRAVUE THRESHOLD FAQs**

[HOW CAN I SEE A THRESHOLD SETTING?](#)



## KNOWN SWITCH ISSUES FAQs

[HSRP - Hot Standby Redundant Protocol](#)

[CISCO CATALYST BROADCAST STORM PROTECTION](#)

[CISCO 2950](#)

[HIRSCHMANN](#)

[HEWLETT PACKARD PROCURVE 2810](#)

[HEWLETT PACKARD PROCURVE 1810G](#)

[WEIDMUELLER IE-SW22/2F-M V4.9](#)

[GARRETCOM](#)

[RUGGEDCOM](#)

[DELL POWERCONNECT](#)

[CISCO IE3000, IE4000, C3600 Series, C3800 Series Switches](#)

## GENERAL FAQs

**Q: WHY DOES A BLANK WINDOW OR NO WINDOW APPEAR WHEN I CLICK ON A MENU ITEM?**

A: The most frequent cause of this is a setting in your popup blocker. Allow the site 127.0.0.1 and/or the IP address of the IntraVUE host machine in your popup blocker configuration. On many machines, the IntraVUE host must be added to Trusted Sites on the Security Tab of IE's Tools/Internet Options.

*Note: You may have to uncheck 'only use https:'*

**Q: WHY DOES A BLANK WINDOW APPEAR WHEN I BROWSE TO INTRAVUE?**

A: If you are browsing from a remote machine, the Java Runtime Environment must be installed on the remote computer. You may go to the [www.java.com](http://www.java.com) website and download the latest version, or

download a version supplied by IntraVUE, go to <http://1.2.3.4:8765/jre> (change 1.2.3.4 to be the ip of the IntraVUE host computer).

If you have Java 7 installed, open the Java console, go to the security tab. Change the setting from high to medium, especially if you are behind a firewall and the certificate cannot be verified.

Microsoft update behavior changed in 2011 which stops some services from fully starting. The IntraVUE services will try to restart themselves for about 3 minutes but the Microsoft updates that are applied when you see messages such as 'please do not turn off the computer while updates are applied' stop some of the IntraVUE services from starting. In the Windows' services dialog start these services if they are not running: 'apache tomcat etomcat', 'autoip i-server', 'autoip ping daemon', mysql.

#### **Q: HOW DO I GET MORE INFORMATION WHEN THE 'TEST EMAIL' BUTTON DOESN'T WORK?**

A: When you use the test email button and you do not receive an answer, there will be some text in an exception message indicating the specific cause of the failure. For example, refused by SMTP host, invalid user name or password, etc. This message is found in the scanner log file located at ...\\IntraVUE\\log and will be the ivserver\_ (date) \_ (time).out file at the time you pressed Test Email.

A sample of what is generated is below. It was generated by doing a Test Email with the default Email Setup dialog.

The stacktrace line "javax.mail.MessagingException: Unknown SMTP host: smtp.somewhere.com" tells you that the SMTP host, the email service provider, is incorrect or that you cannot connect to it.

0120 100016 event: Device 10.1.1.67 reconnected

0120 100054 event: Device 10.1.1.90 moved from 10.1.1.244:9 to 10.1.1.16:2

0120 100054 event: deleted child node at 10.1.1.244:9

0120 100111 event: 10.1.1.32 Ping Response Threshold Exceeded

0120 100122 received mod request send test email 0 0

0120 100122 send test email

0120 100123 EmailTask runs: IntraVUE has been instructed by the admin to send a test email.  
Please see <http://10.1.1.59:8765/to> [unused]

0120 100123 Unexpected Exception thrown - stacktrace follows:

```
javax.mail.MessagingException: Unknown SMTP host: smtp.  
    at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:1211)  
    at com.sun.mail.smtp.SMTPTransport.protocolConnect(SMTPTransport.java:311)  
    at javax.mail.Service.connect(Service.java:233)  
    at javax.mail.Service.connect(Service.java:134)  
    at javax.mail.Service.connect(Service.java:86)  
    at com.sun.mail.smtp.SMTPTransport.connect(SMTPTransport.java:144)  
    at javax.mail.Transport.send0(Transport.java:150)  
    at javax.mail.Transport.send(Transport.java:80)  
    at database.EmailTask.run(EmailTask.java:76)  
    at java.util.TimerThread.mainLoop(Unknown Source)  
    at java.util.TimerThread.run(Unknown Source)
```

0120 100146 device 10.1.1.67 disconnected

0120 100146 event: Device 10.1.1.67 disconnected

0120 100207 device 10.1.1.90 reconnected

Some fields that could cause an issue are the "Enable Email", "Reply-To-Address in Emails", and "Enable SMTP Authentication"

See [Configure Menu - Email Tab](#)

### **Q: HOW LONG DOES IT TAKE INTRAVUE DO FIND NEW DEVICES?**

A: The answer gets technical. There are 4 speed settings in 'scanner tab' of System Configuration that effect discovery. A 'speed' setting effects the time between outgoing packets and how many devices which never responded to a ping, will be pinged in a scan cycle.

- SLOW - 60 millisecond gap between each outgoing packet and a limit of 20 unknown devices/ARPs per scan cycle.

- MEDIUM - 15 millisecond gap and a limit of 64 unknown devices/ARPs.
- FAST - 4 millisecond gap and a limit of 64 unknown devices/ARPs.
- ULTRA - 1 millisecond gap and a limit of 64 unknown devices/ARPs.



Some old Ethernet devices, e.g. Siemens PLC5, will reset using the Ultra speed settings.

The fast speed is generally safe for these devices but should be tested when safe to do so. 3

ARPs in less than 10 msec is the threshold for these type devices. Check with Panduit IntraVUE Support to learn more.

A scan cycle is the time to do all the messages above, wait 2 seconds for replies, send a second round of data based on initial results, wait another 2 seconds, and process the final results. It is nominally 6 to 10 seconds in networks of less than 256 devices, and can be up to 25 seconds for networks bigger than 700 devices.

Take the total possible devices in your scan ranges and subtract the number of found devices. Divide that by the value above and that is how many will be found in one 10 - 15 second scan cycle.

In a class C with 100 found devices, there would be 155 unknown ip addresses and it would take about 8 scanner cycles to get thru the list one time at SLOW and 3 at any other speed.

In a class B subnet, mask 255.255.0.0, with 65,000+ possible addresses it will take more than 1000 scan cycles to go through the list one time when faster than SLOW. If the scan cycle time were 15 seconds, it would take a little over 4 hours to go through the list one time.

### **Q: WHAT ARE AUTO INSERTED NODES (N/A IN IP VIEW)?**

A: With Ethernet, only one physical wire can attach any two devices. When IntraVUE scans a network it finds all the port-for-MAC information available.

An extreme example would be a network with no managed switches. In this case IntraVUE would not find any devices (MAC addresses) being claimed by any switches. Physically all these devices cannot be directly connected to the IntraVUE host computer. IntraVUE reasons that there must be SOMETHING between the host and all these devices. An auto-inserted node represents that device - it could be an unmanaged switch, a hub, a managed switch with an unknown community, and devices on the other side of a router.

Another example would be a single managed switch removed from the host computer by several layers of hubs/unmanaged switches. In this case all the devices further away from IntraVUE will be shown on the ports of the managed switch. All the devices 'closer' to the IntraVUE host will be reported on the uplink port of the managed switch. Since there are no other managed switches to claim these devices and clearly these devices are not all attached to the IntraVUE host, an auto inserted node represents whatever these devices are connected to.

If one of the children of an auto-inserted node is an unmanaged switch, you can configure it as an unmanaged switch in its Device Configuration dialog. It will then take the place of the n/a node and all the 'peers' or adjacent devices will become *its* children.

### **Q: WHAT DOES THE RED MESSAGE 'DATA OUT OF DATE' MEAN?**

A: It means the scanner is no longer active although the network is not in off-line mode. The message appears if the browser has been up for 3 minutes or more and the last threshold sample is older than 3 minutes from the current time. If you right click on a connecting line, there will be a data/time stamp under each threshold graph telling you the last time the scanner was active. The most common cause is that the mysql or 'autoip i-server' service has been stopped or has not started. If starting the services does not solve the problem, please contact tech support at [techsupport@panduit.com](mailto:techsupport@panduit.com) or click 1-866-405-6654.

### **Q: I HAVE A 16-PORT SWITCH. WHY DOES INTRAVUE SHOW PORT NUMBERS LIKE 35 OR 958?**

A: This happens when "stackable" switches are stacked. The firmware in the stacked switches use a method to determine port numbers. IntraVUE reports the same numbers as the switch reports. It may also happen in some routers (layer 3 switches) that also do layer 2 switching. IntraVUE supports a file that can change the port numbers displayed to the user. Visit [www.panduit.com/intravuesupport](http://www.panduit.com/intravuesupport) and search for 'Handling Trunking in Switches'.

### **Q: CAN NON-ETHERNET DEVICES BE DISPLAYED IN THE INTRAVUE SOFTWARE?**

A: Yes, because IntraVUE works on the premise of IP identity, you will have to manually add any device that is not detected or which not respond to pings. This is useful for full visualization and the topology of the network.

Login as administrator and select Add Child from the System Menu on a device that will be the "parent" of the non-Ethernet device. This adds a new node that is a user node, such as a Device Server (Serial to Ethernet converter).

Another example is a PLC with a serial port connection to the Device server. This allows the user not only to view the Ethernet device but also the connected device. The PLC would be able to have a device property and even Web Links (via proxy) without the device containing an embedded Ethernet port.

To be clear, the actual properties of the PLC would not be "viewable"; but IntraVUE could be used to show what is connected to the Device Server and information (such as html files) could be associated with the manually inserted device. A field bus to Ethernet device can also be manually inserted in this manner.

Another example are media converters, such as copper to fiber and fiber to copper. In this case you would probably want to add two manually inserted devices, one attached to the other, and then move the IP device to the last manually inserted node.

There is an excellent video showing this process in action at [IntraVUE Videos](#).

## **Q: WHY DOES ALL THE THRESHOLD DATA GO TO ZERO SOMETIMES?**

A: There are several possible causes of this. If one of the ones listed below does not work for you, please contact at Tech Support at [techsupport@panduit.com](mailto:techsupport@panduit.com) or call 866-405-6654.

If you have hundreds of devices that have been discovered and you have set the scanner speed to SLOW in the System Configuration's Scanner tab, the delays that are inserted between each request the scanner sends may cause the time to collect data to exceed 30 seconds. This will cause the symptoms discussed below. Try setting the speed to medium before changing mysql. (If you have over 500 devices you may have to go at least FAST.)

Bandwidth data is stored in devices as a cumulative number. Any time an APPLY operation is done in the IntraVUE dialogs the scanner re-reads the IntraVUE database to get the change made by the

admin. This causes the scanner to lose its stored value for the last cumulative bandwidth data. The result is there will be no bandwidth data for the minute in which an APPLY operation is done.

### **Q: HOW CAN I SET ALL OR MANY DEVICES TO BE ENABLED FOR EMAIL ALARMS?**

A: By default email alarming is not enabled. You must enable email alarming and setup IntraVUE for the email server in the System Configuration dialog's email tab. Once you have done that you must enable any device you want to receive email alarms about in its Device Configuration dialog. By default the checkbox 'Enable Alarms to Default User' is not checked.

NOTE: *The only event currently sent by email is a device disconnect.*

Use Import/Export and open the exported data in a spreadsheet program. Go to the far right of the spreadsheet and there will be many columns for data located on the general tab of Device Configuration.

Sort the spreadsheet in a convenient way, then set a 1 in the 'SendToDefaultUser' column for any device to be enabled for email Save the spreadsheet as a .csv file and then import it back into IntraVUE.

### **Q: WHY DO THRESHOLD VALUES GET SMALLER WHEN I LOOK AT OLDER DATA?**

A: The 3 and 6 hour data is data based on collecting data once a minute. The bandwidth data is collected at the 0th second of each minute and at the same time the 6 to 15 ping samples (response and failure) within that minute are averaged to become one data point.

So that the database does not quickly become large, after 360 one minute data points, we take the last 10 and record their average and the peak value as one 10 minute sample. This is the 15 and 30 hour data.

When we have 360 of those, the last 12 10 minute samples become one 2 hour sample with the average and peak

values during that period, this is the 15 and 30 day data.

So in the 15 or 30 day graph, one data point is actually 12 10-minute averages made into one statistic, and each one of those had previously represented the average of 10 one minute samples.

## Q: HOW CAN I STOP AND START INTRAVUE SERVICES ON MY LAPTOP?

You can stop the remaining services from a DOS command prompt as shown below.

```
net stop mysql
```

Tomcat and mysql are required to view off line databases but the other services are not.

A: The Intravue Ethernet/IP scanner uses a connectionless UDP message to request the identity of the target devices. The actual request is the CIP IDENTITY message  
6300.

- 388 -



There should thus be no problem with these requests coexisting with normal operational use of even an Ethernet/IP device with limited connections, those devices normally support message repetition rates exceeding 100 per second.

## INSTALLATION AND SYSTEM REQUIREMENTS FAQs

### **Q: WHAT ARE THE RECOMMENDED SYSTEM REQUIREMENTS?**

A: All Windows Operating Systems are supported except Vista and Windows 8 variants. A virtual machine with one

of the supported OS's will also work.

The VMware vSphere® High Availability environment (and similar solutions from other vendors) is not supported as it creates frequent changes of host environments in a way that causes problems.

4 GB RAM is recommended for more than 500 discoverable devices, 2 GB for less.

Any recent CPU will be fine. IntraVUE will run with as little as 4 GB of disk space but 8 GB is wise if you have more than 1000 devices being scanned.

IntraVUE does not take particular advantage of multiple processors/cores.

The host computer must be able to ping any devices to be monitored.

If devices are not in the same subnet as the IntraVUE host, the host must be able to get SNMP data from the gateway of the subnet to be monitored. This means IntraVUE must be configured with the Gateway/Router's SNMP Read Only community and the host IP must have authorization in the gateway.

If you DO NOT or CAN NOT get SNMP permissions, you can add NIC cards to the host so that the other subnets become local to the host or you can add an IntraVUE Agent.

You cannot currently scan the proxy ip addresses of devices that are on the other side of Network Address Translators (NATs). NATs usually provide its mac address to all the proxy ip addresses and this interferes with some of the IntraVUE scanner's other functions. A solution is in progress.

## Q: HOW MUCH NETWORK TRAFFIC IS GENERATED BY INTRAVUE AND THE INTRAVUE SUPERVISOR?

A: The amount of network traffic (network usage, or bandwidth usage) put on the network by IntraVUE™ is controlled to some extent by the 'speed' setting under Configure > Scanner > Scan settings. On average it is about 0.5 percent.

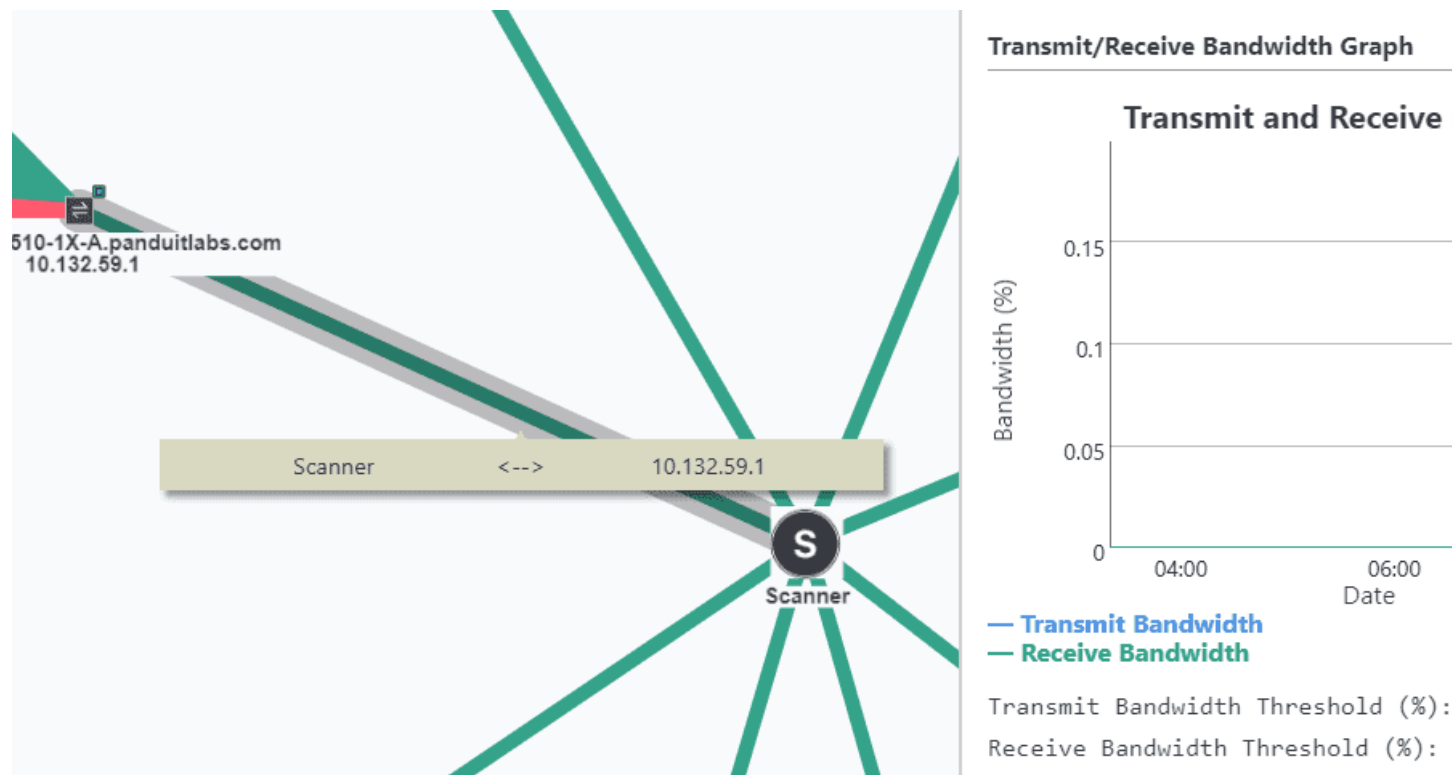
Measurements show the typical load, at the fast setting, for scanning 100 nodes is about 5K bytes/sec or 0.04% at 100Mbps, and load when actively browsing is about 40K bytes/sec or 0.3%. Both of these numbers are likely to scale approximately linearly.

There will be also a broadcast traffic impact of about 200 bytes/sec on average, or 0.002% from the ARP traffic.

This will not increase much with node count (actually will tend to go down as node count increases because the scan rate slows)

### How to Measure bandwidth usage on by Intravue network

Click on a connection link between the scanner node 'S' and its closest fully managed switch to determine the bandwidth use of that entire network.



### **Q: WHAT PORTS ARE USED BY INTRAVUE?**

A: Make sure that the following ports are not being blocked from the IntraVUE host machine to all devices in the scan range by a Firewall/ASA router, Access Control List (from an L2/L3 Switch or Router), or Deep Packet Inspection/IDS/Security appliance?

#### **TCP ports**

80 - used to find devices with web pages and to provide a link to those pages automatically. May also be used as additional port to browse to IntraVUE if it does not conflict with IIS.

8765 - mandatory port to browse IntraVUE

#### **UDP ports**

161 - used for SNMP

162 - used to listen for SNMP trap messages

137 - used to find NetBIOS names

44818 - used for Ethernet/IP CIP protocol

65402 - used for communication to IntraVUE Agents

65403 - used for communication to IntraVUE Agents

## **CONFIGURATION QUESTIONS**

### **Q: IS THERE AN EASY WAY TO ADMIN VERIFY ALL THE DEVICES?**

A: Selecting each device and using the Device Configuration dialog can take a long time.

Go to the Scanner Tab of the System Configuration dialog and select the button 'Admin Verify All Devices'. This will verify everything except the auto-inserted (n/a in IP view) nodes. If the n/a nodes really represent hubs they should be individually admin verified and given names.

### **Q: WHY ARE ALL OR MOST THE DEVICES UNDER AN UNRESOLVED NODE?**

A: As soon as a device responds to a ping request it is added to the unresolved node of that IntraVUE network.

Note: a bug from version 2.1.0b to 2.1.0b17 existed that sometimes prevented a device from appearing.

The scanner then tries to find the mac address for the top parent or any device it can identify as a router that is configured for SNMP. If you look at the properties for a device under unresolved and you do not see a mac address, you have probably selected the wrong top parent, the wrong router, or not included the router that "owns" the device.

There should be a green outline around any routers. If not the snmp is not configured correctly in IntraVUE or the router. The router may use Access Control Lists and the IntraVUE host is not in the list.

Try using the DOS command "tracert x.x.x.x" using the ip of a device in unresolved. The last router in the resulting list must be in the scan range and may have to be the top parent for that network.

IntraVUE Help has a good description of selecting the right top parent.

#### **Q: I HAVE MANY INTRAVUE NETWORKS, CAN I ONLY SHOW ONE OR TWO AT A TIME?**

A: There are two options that can be added to the URL used to browse to IntraVUE. The URL that will be in the address bar of your browser after launching IntraVUE is <http://127.0.0.1:8765/iv2/i-vue.jsp>.

To hide networks use ?h= and a comma separated list of networks to hide.

Example: <http://127.0.0.1:8765/iv2/i-vue.jsp?h=1,3> hides network id 1 and 3.

To ONLY show network that you, instead of hiding them, use ?n= and a comma separated list of networks to show.

Only those networks listed will appear.

HINT: To easily tell the network numbers look at the Network panel in the Event Log's Show Filters mode. In the Network list box, the network number appears with each network name.

#### **Q: CAN INTRAVUE SCAN THROUGH A FIREWALL AND IF SO, HOW?**

A: First, we recommend you DO NOT scan through a firewall. The ping data will include delays and characteristics of the router which are not seen on the other side of the firewall. There will also be unnecessary traffic going through the firewall. We recommend an IntraVUE be installed on the far side of the firewall and that you browse remotely to it. If that is not possible, you can set up the firewall to allow certain traffic from the IntraVUE host computer to pass through the firewall to the target sub-nets.

The traffic which must be carried through a router or firewall for IntraVUE to work is as follows:

### **ICMP request and response (so that PING works)**

### **UDP port 161 (SNMP)**

In addition, if the firewall is used for routing, the firewall itself must have SNMP switched on, and must publish the ARP table as if it were a router. The ARP data is where IntraVUE determines the MAC address of each target. In most cases, firewall appliances do not satisfy this condition, which is why IntraVUE cannot normally see devices on the other side of a firewall. Or it may be possible but IT will refuse to allow it. You can determine if the firewall has routing responsibility by using TRACERT to a device in the target scan range. If the firewall is listed as one of the 'hops' then it is being used as a router.

The ARP data from the 'last hop' router must be available to IntraVUE. This is by configuring the READ ONLY SNMP community. If the firewall is the last hop, then SNMP must be available to IntraVUE. Otherwise it will be a similar situation to forgetting to add a router to the scan range. IntraVUE will be able to determine if target devices themselves are 'up' or 'down', but will not be able to determine the topology (All devices will stay in 'Unresolved'). The user can compensate for this by using 'manual moves' but this is usually less than ideal.

It is highly recommended that the IntraVUE scanner be on the same side of the firewall as the target devices to be monitored. Much of the topology and performance data available through IntraVUE will be degraded if the scanner is remote.

### **Q: CAN I BACKUP INTRAVUE FROM A DOS COMMAND PROMPT?**

A: YES you can, although do not use the mysql utility mysqldump. If you use that you will back up some database tables that will cause problems if you were ever to restore the database.

Some IntraVUE users have wanted to make backups every 6 hours. In this way they will always have a backup to restore that will have threshold data using 1 minute resolution for pings and bandwidth.

The IntraVUE backup from the System Configuration dialog can be accessed, but commands are complicated.

The commands below can be pasted into a batch file.

The batch file will create a backup having date and time information in the filename, so no parameters to the batch file are required.

The SET commands at the end can be changed if you have installed components in a different location.

```
set ctime=%Time%

set cdate=%Date%

for /f "tokens=1,2,3 delims=:" %%a in ("%ctime%") do (

set chour=%%a

set cmin=%%b

set csec=%%c)

for /f "tokens=2,3,4 delims=/ " %%a in ("%cdate%") do (

set cmon=%%a

set cday=%%b

set cyear=%%c)

SET IntraVUE_Dir=c:\\IntraVUE

SET APACHE_DIR=%IntraVUE_Dir%\\autoip\\tomcat8

SET MYSQL_DIR=c:\\mysql

java -cp "%APACHE_DIR%\\webapps\\livConfig\\OrgNviUtil.jar;%APACHE_DIR%\\-
common\\lib\\mysql-connector-java-3.0.14-production-bin.jar" IntraVUEBackup %MYSQL_
DIR%\\bin netvue netvue "%IntraVUE_Dir%\\d-
bBackup\\backup_%cyear%-%cmon%-%cday%-%chour%.%cmin%.%csec%.dmp"
```

### **Q: HOW CAN I GET BETTER PORT NUMBERS FOR CISCO SWITCHES THAT ARE STACKED?**

A: Technically, the port number reported by IntraVUE is the port number that is returned from the switch's bridge mib. A port number is translated into an interface number and the switch maintains information about the port and interface using numbers that do not always relate to what you see on the front panel of a switch. Normally port 3 is interface 3 and that agrees with the front panel. When switches are stacked, you may find a port number like 193 or even 1103 on a 48 port switch.

Cisco has a special mib entry that provides stacking information and this is supported by a few other manufacturers. If this was a standard mib entry, IntraVUE would use it but because it is different or doesn't exist between manufacturers we do not. The IntraVUE tools folder (c:\\IntraVUE\\tools) contains several batch files.

One is 'snmpwalk.bat'. You can use that to query a Cisco switch and get some information that looks like the sample below.

The syntax is:

```
snmpwalk ip_address read_only_community 1.3.6.1.2.1.47.1.1.1.1.7
```

For example:

```
snmpwalk 10.1.1.244 public 1.3.6.1.2.1.47.1.1.1.1.7
```

For one of our Cisco switches the response is:

```
1.3.6.1.2.1.47.1.1.1.1.7.1: "Cisco_Switch"
1.3.6.1.2.1.47.1.1.1.1.7.2: "FastEthernet0/1"
1.3.6.1.2.1.47.1.1.1.1.7.3: "FastEthernet0/2"
1.3.6.1.2.1.47.1.1.1.1.7.4: "FastEthernet0/3"
1.3.6.1.2.1.47.1.1.1.1.7.5: "FastEthernet0/4"
1.3.6.1.2.1.47.1.1.1.1.7.6: "FastEthernet0/5"
1.3.6.1.2.1.47.1.1.1.1.7.7: "FastEthernet0/6"
1.3.6.1.2.1.47.1.1.1.1.7.8: "FastEthernet0/7"
1.3.6.1.2.1.47.1.1.1.1.7.9: "FastEthernet0/8"
1.3.6.1.2.1.47.1.1.1.1.7.10: "FastEthernet0/9"
```

The last number in the string of numbers is typically, but not necessarily, the port number that will appear in the IntraVUE browser. For more info, see Cisco's web site [browse OIDs](#).

You may use this information to modify what IntraVUE shows you using the IntraVUE system file, trunkingdefs.txt in the ..\IntraVUE\autoip folder. Refer to the IntraVUE help file and look for 'handling trunking' as the last item in the Admin section. You can also add this information as a second line in the 'hover text' that appears when you are over a connecting line, see the end of 'Hover Feature' in the User section of Help.

#### **Q: HOW DO I CHANGE THE PASSWORD FOR INTRAVUE?**

A: To change the default "intravue" password see for more details

## **DIAGNOSING NETWORK ISSUES**

#### **Q: WHAT IS CONSIDERED A PING FAILURE?**

A: The IntraVUE scanner pings discovered devices nominally about 10 times per minute. At the end of each minute bandwidth statistics are collected from SNMP devices and the results of pinging during that one minute are averaged. For each minute, for each device, there is one value for transmit and receive bandwidth, ping response, and ping failures.

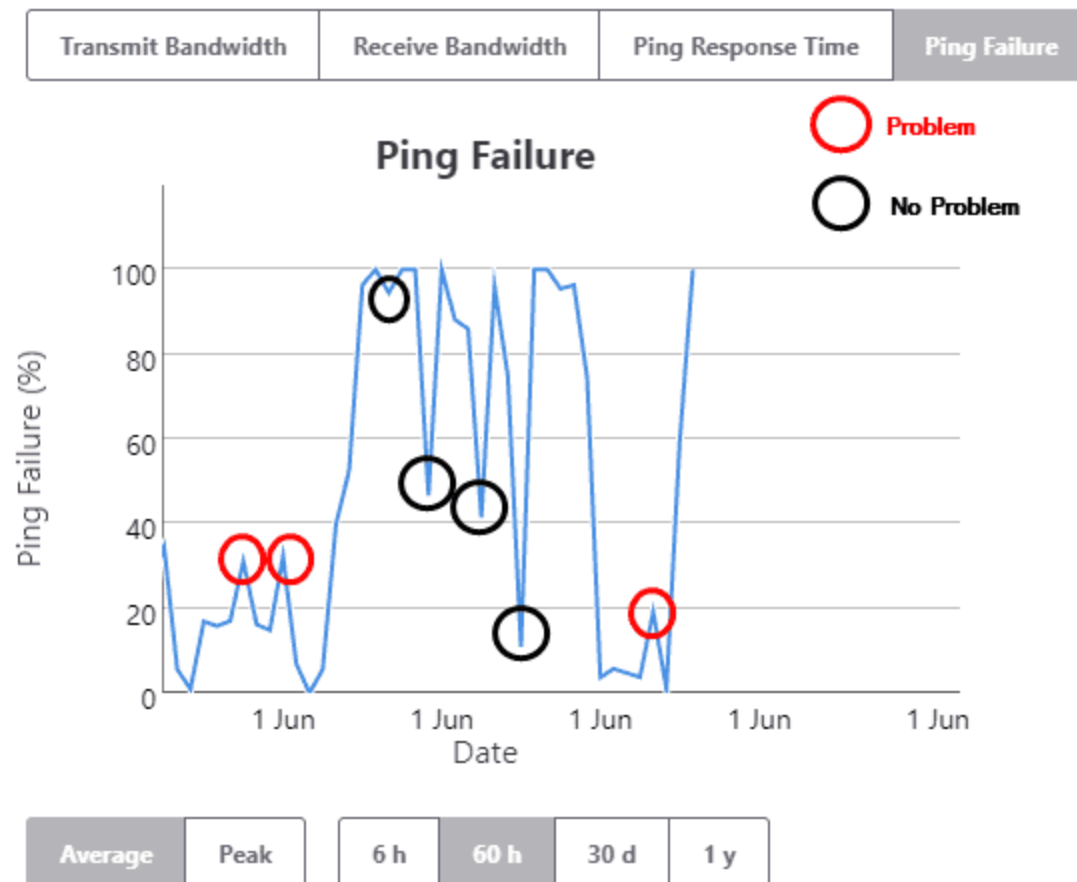
Within each one of the 10 or so 'scanner cycles' per minute, the scanner pings every device and waits for 2 seconds. After the 2 seconds it checks for all the responses. If a device fails to respond, a new ping is sent immediately. If a device still does not respond it is logged as disconnected. If it DOES respond, a ping failure is recorded. The ping failure rate is a percentage: (the number of ping failures) divided by (the number of pings in that minute).

#### **Q: WHAT IS NORMAL VS DISCONNECT?**

A: If a device is disconnected, it will have a 100% ping failure rate during the minutes it was disconnected for the full minute and usually some percentage during the minute it disconnects and



reconnects. *These ping failures are normal and are NOT a concern.* In the image below, ping failures with a black square are normal. Those circled in red indicate a problem.



Some Causes of Ping Failures Include:

- 🕒 Ethernet cable connector bad or loose.
- 🕒 Ethernet cable crimped or damaged between end points.
- 🕒 Ethernet cable effected by environment such as motors starting, weight on cable.
- 🕒 There is a long cable and the switch and the device negotiated a high speed during auto-negotiate but due to the length there are occasional problems. Manually set a lower speed if possible on both ends.
- 🕒 Device is too busy with main tasks to respond to pings.
- 🕒 Mismatch of speed/duplex settings between device and switch.

- 🕒 Switch and device set for auto-negotiate but device has problems negotiating. Set both devices to have the same settings without auto-negotiate.
- 🕒 Device responds, but longer than the 2 seconds the scanner waits for a response.
- 🕒 Poor or inexpensive design of device, such as a bar code reader.

## **Q: HOW DO I DIAGNOSE PING FAILURES?**

A: If there are several devices having problems and they are on the same switch, check the switch. Many of the causes are due to the cable in some way. Check to be sure the cable is fully seated on both ends. In most plants replacing the cable is a difficult task. You can determine if the cable is the problem with several techniques.

If another device is nearby and it is not having problems, swap the cables at the device end and see if the problem also moves. You can use a hub and a second, known good cable if you need extra length.

Another technique is to take a known good device of any type and install it next to the device having problems. Put a known good hub at the end of the cable being tested and connect the problem device and the known good device into the hub. If only the problem device is having failures, it's the device itself.

Check the settings for speed, duplex, etc. in both the port of the connected switch and the device. Resolve any differences. If one or both are set for auto-negotiate, set them both to a No setting that is NOT auto-negotiate. If the cable length is long, set them for a lower speed to see if the problem goes away.

You can install a packet sniffer, such as WireShark, on the IntraVUE host computer and find out if the device is responding, but responding longer than 2 seconds. IntraVUE can be configured to for a longer wait period but this will effect everything done by the scanner. It should only be done after consulting with tech support.

Finally, it may just be the nature of the device. If the operation of the device is good and it is not affecting operations, you will have to learn which ping failures are significant and which are not.

## **Q: HOW ARE DUPLICATE MAC ADDRESSES DISPLAYED?**

A: A MAC address is supposed to be unique in the world. They are assigned by device manufacturers and are not intended to be changed. Switches move packets between their ports by inspecting the header of the packet. A destination MAC address will be in the header. The switch then looks up the port number assigned to the MAC address in its 'bridging table'. The message is then sent out of that port. This is done without regard to the IP address information in the packet. (Only routers pay attention to IP addresses.)

Duplicate MAC addresses in a network typically cause messages to FAIL to be delivered to the correct location, resulting in lost or intermittent communication to the affected pairs of devices.

A switch will remember a port number for every MAC that was in a recently received packet. A device sending a message would have found the MAC address for the IP as a result of sending a broadcast ARP request and having the response come back through all the switches in the path to the target device.

In the case of duplicate MAC addresses, the port for a mac may be the one leading to IP address X or it could be the one leading to IP address Y. It will depend on the last traffic received by the switch. So if the switch receives a packet intended for device X, but a recent packet received at the switch was from device Y with the same MAC, the switch will transmit the packet on the incorrect port. The IntraVUE scanner examines the ARP caches it knows about and when it sees that a MAC address is associated with a new IP address, the IntraVUE database is updated to reflect this change, and an event log entry is added. This is necessary to handle the case where a device has been reconfigured to change its IP address. However, when there are DUPLICATE MAC addresses on a network, such event log entries may also be seen, often in conjunction with an apparent 'move' of the device.

In the image below you will see a similar situation where two devices have the same MAC. (The part of the event log displayed below is when the duplicate MAC first starts to occur.)

***NOTE: In the case of duplicate macs, the IntraVUE event log will record frequent, several times a day, changes in location for the devices that have the duplicate.***

Topology Plant Layout **BETA** Device List Filters **Event Log** Diagnostics

changed ip				
ID	Date/Time	IP Address	Description	
!	4554	Jun 1, 2015 4:12:00 PM	<a href="#">10.1.1.80</a>	Device 10.1.1.195 (F0 AD 4E 00 49 3F) changed IP to 10.1.1.80
!	3050	Jun 1, 2015 9:55:46 AM	<a href="#">10.1.1.43</a>	Device 10.1.1.56 (00 18 A9 00 06 6F) changed IP to 10.1.1.43

Right after the device with the duplicate mac joins the network, IntraVUE records that the original device has changed its IP address based on information provided by ARP requests. At this point the original device now has the IP and other info of the new device. The original device then responds to its original IP and it is added as a NEW device, then the duplicate MAC is detected, and the process continues in an endless cycle; until the problem is fixed.

Because layer 2 switches deliver data based on MAC address packets intended for either of these devices often end up at the other device. If you look at the line threshold graph for either device you will see many ping failures - almost constantly.

This is because the ping intended for one of the IPs takes the path to the other IP and the other IP does not respond. See [Connection Side View](#)

## Q: HOW ARE DUPLICATE IP ADDRESSES DISPLAYED?

A: Getting duplicate IP addresses on a network is fairly common. If someone gives a device a fixed IP and gets the IP by looking for a device that doesn't respond to a ping, when the disconnected device powers on you will have duplicate IPs.

*NOTE: Using the IntraVUE search function to find IPs that don't exist will guarantee an IP has not been used since the scanner was started.*

When there are two devices with the same IP address in a subnet, both will hear broadcast messages asking 'who has ip address X?' and both will respond 'I do, my MAC is ...'.

Each device will have a different MAC. Each switch that the response is returned through will have that MAC assigned to the appropriate port for the IP that responded.

When a device issues an ARP request to find out 'who has an IP' the most recent response will overwrite any previous responses in the device's ARP cache. Messages will be formed using that MAC address. Switches will route the message by port for that MAC address (switches don't consider the IP address in the packet). When there are duplicate IPs the MAC address that the IntraVUE scanner will associate with a device will change over time depending on the sequence ARPs are returned.

changed mac				
ID	Date/Time	IP Address	Description	
!	954038	Dec 6, 2017 2:15:27 PM	<a href="#">10.132.56.92</a>	Device 10.132.56.92 changed mac from 00:50:56:b4:7
!	954019	Dec 6, 2017 2:15:27 PM	<a href="#">10.132.56.92</a>	Device 10.132.56.92 changed mac from 00:50:56:b4:7

Additionally, IntraVUE associates a MAC with an IP and when a switch reports the 'new' mac of an IP is at a different location in the network, IntraVUE will move the device to its 'new' location.

The result will be frequent events about a device IP having a new MAC address and the device moving. The moves will alternate between the two physical locations of the devices in the network.

By following the Ethernet cable connected to the ports of the managed switches the devices are moving between you will find the devices with the duplicate MACs. (You do have managed switches don't you?).

See also [Event Logging](#)

### Q: I CAN PING A DEVICE FROM DOS, WHY DOESN'T INTRAVUE DISCOVER IT?

A: A ping request packet (ICMP protocol) contains an identifier. The identifier tell which request packet is being responded to.

When DOS issue a pings every outgoing packet contains the same identifier, 1.

When IntraVUE issues pings each packet has a different identifier so the time to respond is accurate and not a late response to an earlier ping is not confused with the one just issued.

Some device implementation of the ICMP protocol (ping) just copy the DOS response and always respond with the same identifier. The result is that the ping response is analyzed by IntraVUE, the

identifier does not match, so the response is ignored. This makes the device undiscoverable by the IntraVUE scanner.

Some devices do not copy the data payload of the request into the data payload of the response over a certain size. The ICMP spec requires responses of many thousands of bytes. The devices that fail typically only handle up to 32 bytes, the same size as a DOS ping request's data payload.

To test this case you can force a packet size in a DOS ping, try these example pings. If the ping fails, that is why IntraVUE is not finding the device or shows it as disconnected.

```
Ping 10.51.11.160 -l 35
```

```
Ping 10.51.11.160 -l 1025
```

Devices known for this behavior include...

- Honeywell UDC 2500
- Infinias badge readers

## **Q: CAN INTRAVUE SCAN MESH NETWORKS?**

A: Yes, but it depends on what you define as 'scan'.

At the lowest level, Intravue can 'scan' any network which contains devices which respond to PING and Intravue will correctly indicate when such devices connect/disconnect and will monitor the ping response and ping failure rates. This means that even without topology support, there is a valid business case for Intravue scanning. Many customers in fact use Intravue just like this, typically because the networks they are monitoring use switches which are not 'SNMP managed'.

In order for Intravue to provide meaningful automatic topology determination and placement, the infrastructure switches need to provide reporting using the 'Bridge MIB' (RFC 1493) and there needs to be read-only access provided to the Layer 2 and Layer 3 switches involved.

Many 'mesh' arrangements where switches are connected to multiple other switches (including multihoming) there are alternative paths for messages to propagate from device to device. When using such systems the Intravue topology determination can appear to change often or can fail to complete (Intravue will not make a 'move' of a device if there is conflicting information about where the device is located).

In these circumstances it may be preferable to disable the SNMP reporting from the switches concerned, rather than try to 'fix up' the topology by using trunkingdefs files.

So there is no requirement that Intravue avoids MESH networks, just that the more similar the network is to a 'traditional' layer 2 switching arrangement using SNMP managed switches, the more valuable and accurate the topology reporting is likely to be.

## MySQL

### **Q: THE MYSQL FOLDER HAS GIGABYTES OF DATA, HOW TO I MAKE IT SMALLER?**

A: Your C:\\MySQL\\data folder may contains files that start with "mysql-bin", like mysql-bin.0000005. These files are used by mysql for transactions when Windows' resources are low in a feature not used by IntraVUE.

You should comment out two lines in the c:\\MySql\\my.cnf file. It is usually best to open WordPad and then use File/Open to edit the file.

Put a # sign in front of the two line as shown below.

```
# log-bin=mysql-bin
```

```
# binlog_format=mixed
```

Now stop the mysql service using the Windows Service dialog. This will cause the autoip i-server service to also stop.

Delete all the mysql-bin.0000xx files in the mysql\\data folder and start the mysql and autoip i-server services. The files will not be created anymore.

Note: Starting with IntraVUE version 2.1.0c5, these lines are commented out of the my.cnf file if you chose to replace mysql.

### **Q: CAN I EXPORT EVENTS FROM THE EVENT LOG?**

A: You may wish to look at IntraVUE events in a text file or spreadsheet. You can do so from a DOS command prompt. It is easiest if you run the DOS command prompt in the c:\\mysql\\bin folder where you can omit the beginning c:\\mysql\\bin\\.

The basic syntax to show the results on the console is:

```
c:\mysql\bin\mysql IntraVUE -uroot < filename.sql
```

You may need to add the user and password to the command line depending on which version of IntraVUE you have. If this is the case, please contact tech support for the correct syntax.

The basic syntax to save the results in a file (redirect) named save\_file.txt is:

```
mysql IntraVUE < filename.sql > save_file.txt
```

You can create several .sql files to get different events from IntraVUE.

To get all events sorted by IP address, create a new .sql file with notepad having one line. The RPAD forces the results to have a certain number of spaces.

```
SELECT RPAD(EventId,5," "), RPAD(Occurred,21," "), RPAD(IpAddress,16," "), Description  
from event ORDER BY IpAddress, EventId;
```

To get all events into a CSV file (don't use the redirect command line for this one) (Note: modified 1/3/2013) Note: the csv file will be saved in the mysql\data\IntraVUE folder.

```
SELECT * from event INTO OUTFILE '130103_events.csv' FIELDS TERMINATED BY ','  
OPTIONALLY ENCLOSED BY '"' LINES TERMINATED BY '\r\n';
```

#### **Q: IT IS POSSIBLE TO COMBINE THE SQL FILE AND THE DOS COMMAND INTO A SINGLE BATCH FILE AS SHOWN IN THE FOLLOWING EXAMPLE?**

A: The ">" from the command line becomes a "-e" option in the batch file. Avoid double quotes except after the -e and at the end of the line. To get all events between two dates, create a batch file and copy the lines below into the batch file. Modify the START and END dates as appropriate.

```
REM set the dates for the report below.
```

```
REM They report will be called "ivEvents_startdate_enddate.csv"
```

```
REM In your spreadsheet program select semi-colon as the separator, not comma.
```

```
SET START=2012-12-09
```

```
SET END=2012-12-17
```

```
c:\mysql\bin\mysql IntraVUE -uroot -e "select eventid, ';', occurred, ';', class, ';', description from  
event WHERE occurred > '%START%' AND occurred < '%END%' order by eventid ASC" >  
ivEvents_%START%_%END%.csv
```



### IntraVUE™ AND SYNAPSENSE

#### **Q: CAN INTRAVUE AND SYNAPSE RUN ON THE SAME MACHINE?**

A: YES. SynapSense has researched the conflict between IntraVUE™ and with older SynapSense 2.4Ghz systems and there is a way to change the default 3306 MySQL port for SynapSense. Newer SynapSense offerings (e.g. SynapSense 900) are not subject to this same conflict. Contact tech-support@panduit.com for more information.

### Modbus/TCP

#### **Q: IS THERE A TOOL AVAILABLE TO HELP DEBUG MODBUS ISSUES?**

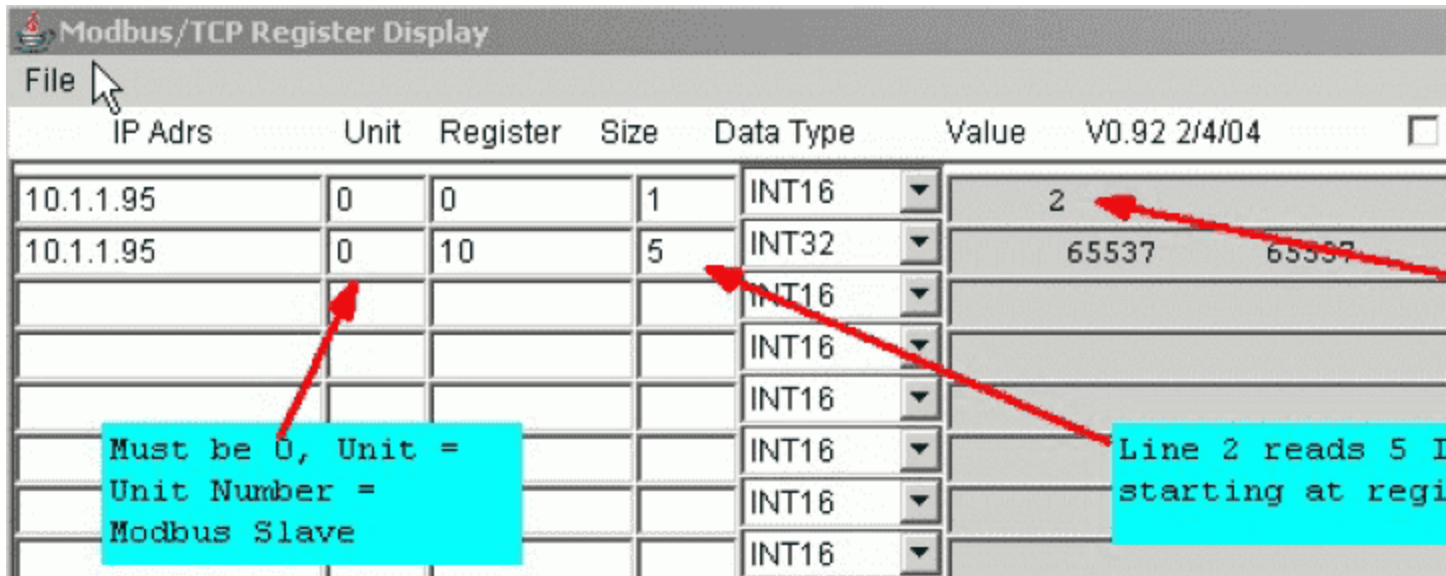
A: A modbus monitoring tool is available to help diagnose problems with modbus/tcp. This tool is from the

modbus.org web site. The tool is a modbus client that can be directed at a modbus server, such as the IntraVUE

host computer on port 502.

Double click the .jar file to launch it (requires a JRE on the host) and enter the IP address of the IntraVUE host. Use

127.0.0.1 if you are running from the host.



Set unit to 0.

Note: IntraVUE versions after 2.0.3 responded to all unit ids.

Set register to 0 to start at the beginning, size to 10 for 10 data types per request, and datatype to INT16.

## THRESHOLD (PING, PING FAILURES, BANDWIDTH) FAQs

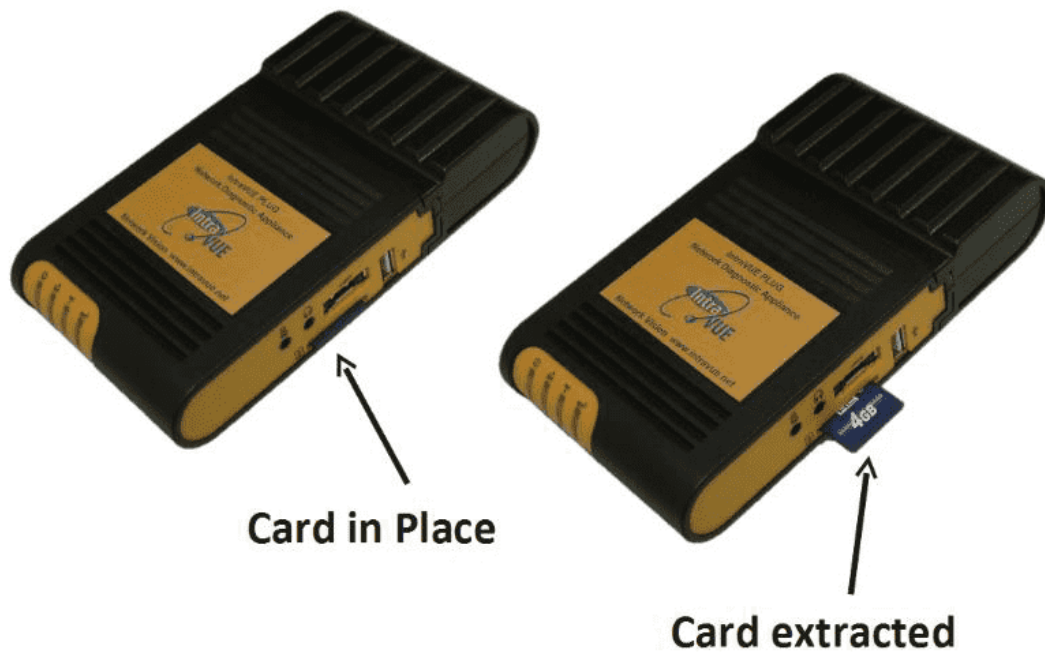
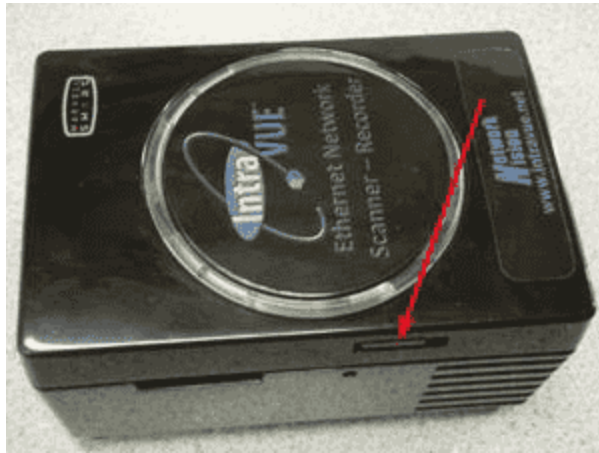
### Q: HOW CAN I SEE A THRESHOLD SETTING?

A: By positioning the mouse over a connecting line and right clicking. A threshold dialog box associated with the two connecting devices will open. You can view the thresholds from here. The administrator sets the default thresholds in the Threshold Tab of the System Configuration dialog. The values are assigned upon device discovery. Threshold values are the limits that change line colors from green to yellow in the main display. The values are retrieved from the data stored in the database. The administrator can change the current threshold values for an individual device in the threshold dialog itself.

## PLUG AND APPLIANCE FAQs

**Q: HOW DO YOU REPLACE THE MICRO SD MEMORY CARD?**

A: The Operating System of the IntraVUE Plug is contained on the micro SD card. The micro SD card contains all data except registration and network addresses.

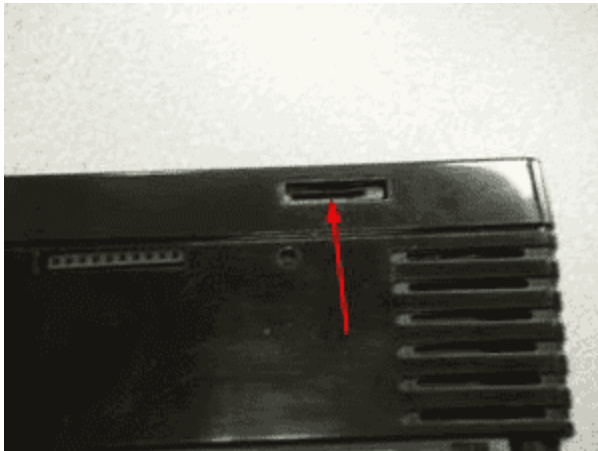


The micro SD card is located on the left side as viewed from the 'top'.

**Removal** is done by pushing the card further **INTO** the plug, you will feel some spring-like resistance, and then releasing. The card will then 'eject'.



**Replacement** is done by inserting the micro SD card into its 'slot'. Be careful to insert the card into the slot, as it is possible to insert it above the slot.



After you push the card **FULLY** into the slot, you will feel some spring resistance, and when you release your finger the card will stay in the slot.

**Q: HOW DO YOU CHANGE/SET THE DATE, TIME, AND/OR TIME ZONE ON THE PLUG?**

A: There are several utilities available on the plug for settings its internal date and time.

By default the plug looks for a time server to provide the time. The default server is set for pool.ntp.org. In most installations this will not be available. If a local time server is available you can set it by substituting its URL for pool.ntp.org in the URL below

`http://(IP OF PLUG):8765/tools/util.jsp?ntpserver=pool.ntp.org`

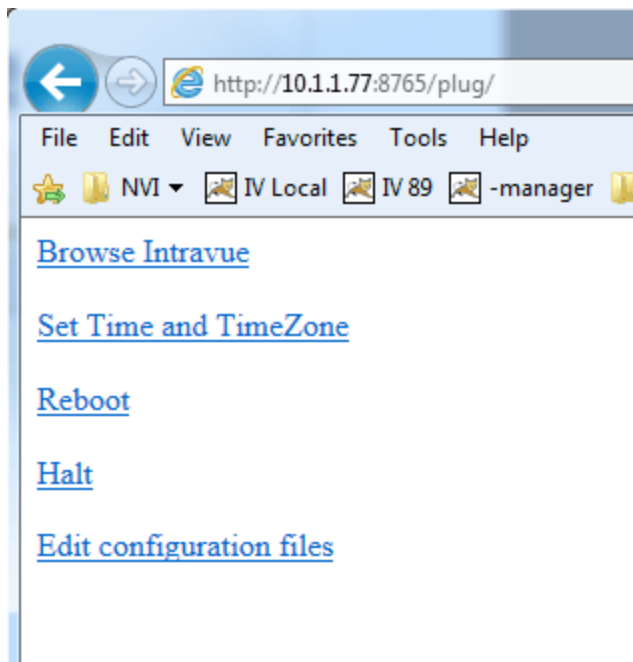
The response should look like this:

`ntpserver pool.ntp.org`

`setting network time server to pool.ntp.org`

To set the time or time zone use the plug's utility page by appending "/plug" after the :8765 in the address you use to access IntraVUE.

If you need to use the plug's internal clock, it is a good idea to start by making sure the time zone set in the plug is the right one for your time zone. The time changes when the time zone changes.



Month:  Day:  Hour:  Minute:  Year:

Please note that the date change will not take effect for up to 60 seconds after pressing Submit  
You can confirm the date is set correctly by re-visiting this page.

Current timezone:   
Time Zone (Continent/City):

Please note that a timezone change will only take effect on next reboot.



**DO NOT CHANGE THE TIME BEFORE SETTING THE CORRECT TIMEZONE  
AND REBOOTING THE PLUG OR APPLIANCE.**

A list of all possible time zones is in the drop down list. Select the one for your location, for instance "Europe/Paris". Once the time zone is correct (reboot if you changed it), you can change the time.

## INTRAVUE & JAVA FAQs

### Q: WHAT MUST BE CONFIGURED BEFORE JAVA WILL WORK WITH INTRAVUE IN MY BROWSER?

A: Starting with Java 7, a security tab has been added to the Java Control Panel, most recently found in Start/Programs/Java/Configure Java. You MUST add the full URL used to launch Intravue as an exception, up to and including the :8765

If you are using Internet Explorer, you MUST also add the URL/IP to the list under the security tab's Trusted Sites

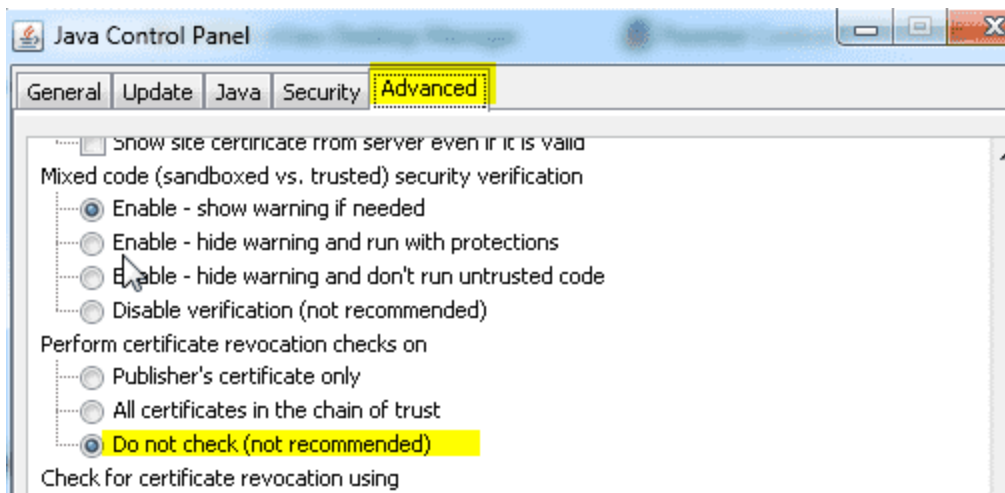
### Q: WHY DOESN'T SEARCH CENTERS A DEVICE IN INTERNET EXPLORER 11?

A: This issue is related to java and security requirements in Internet Explorer 10 and 11. IE is preventing the communication between different pop up windows. To make this work, go to the 'Page' icon in the toolbar, select 'Compatibility View Settings', add the IP of IntraVUE to the list.

### Q: INTRAVUE IN THE BROWSER IS TAKING A LONG TIME TO LOAD, WHY?

A: There is a Java security setting that needs to be adjusted if the browser does not have direct access to the Internet, or you will get this symptom.

- ⌚ control panel : java : advanced : (Note: in the latest Java, this has moved to Start : Programs : Java )
- ⌚ Perform certificate revocation checks on
- ⌚ Do not check (not recommended)



Once you make this change, the delay will disappear.

Basically what is happening is that Java is trying to make sure the 'certificate' is valid. But because there are reasons that a certificate might be 'revoked' (because an employee steals it for example), Java needs to 'ask' the certificate authority to check. But because the computer has no Internet access, this will not work, so it tries for a while and then gives up. Hence the 'delay'.

The workaround is to tell Java to suppress the check, since there is no security risk (you are not attached to the Internet anyway).

## INTRAVUE THRESHOLD FAQs

### HOW CAN I SEE A THRESHOLD SETTING?

By positioning the mouse over a connecting line and right clicking. A threshold dialog box associated with the two connecting devices will open. You can view the thresholds from here.

The administrator sets the default thresholds in the Threshold Tab of the System Configuration dialog. The values are assigned upon device discovery.

Threshold values are the limits that change line colors from green to yellow in the main display. The values are retrieved from the data stored in the database.

The administrator can change the current threshold values for an individual device in the threshold dialog itself.

## KNOWN SWITCH ISSUES FAQs

### HSRP - Hot Standby Redundant Protocol

HSRP allows two Layer 3 Switches (Routers) to be connected and share data. If one router fails, the other will assume all functions of the other. To complete the redundancy, the upper level Layer 2 switches are redundantly connected to each router. This has the potential for network traffic to take different paths at any time, although in practice it happens rarely.

The trunkingdefs.txt file needs to be configured so the Intravue scanner treats the two ports of a redundantly connected switch as being the same port. In Intravue Help, see 'Handling Trunking in Switches'.

In some cases the issue will go away by not scanning both the virtual IP and both physical IPs. If the virtual IP in a subnet is the .1 and the two physical IPs are .2 and .3, the first approach would be to scan the .1's, but not the .2 and .3. The range in each subnet in this case would be in two lines:  
X.X.X.1 to X.X.X.1 plus X.X.X.4 to X.X.X.254

The other approach is to skip the virtual IP and make the scan range X.X.X.2 to X.X.X.254

If using either of these approaches it is very important to be consistent in every Intravue network so the excluded IP(s) are NEVER in the scan range.

## CISCO CATALYST BROADCAST STORM PROTECTION



Cisco can suppress broadcast, multicast, or unicast traffic if the per cent of those packets exceed a certain value. If the percent of traffic goes above a "suppression"™ level, all packets of that type are discarded and the switch then continues to get packets. This is supposed to help but generally hurts when enabled.

A setting of 50 means if more than 50% of the packets are of type X, then discard all packets. A setting of 100 effectively disables the setting, a setting of 0 effectively kills the switch. Note: in some switch software it is called flooding control, in others it is called storm control.

Cisco Note on [Configuring Port-Based Traffic Control](#)

### CISCO 2950

The port numbers on the switch faceplate are the reverse of this switches internal port numbers, the numbers used by Intravue. Port 1 is reported as 12, 2 as 11, etc.

You can edit IntraVUE's trunkingdefs.txt file and have Intravue report the numbers you would expect. This is an example covered in Intravue Help, see 'Handling Trunking in Switches'.

### HIRSCHMANN

Early versions of Hirschmann Mach switches did not report the Bridge Mib (RFC 1493) and instead used the Q-Mib. The Bridge Mib tells the port number for a MAC address, the Q-Mib is a newer standard designed to handle VLANs. The Q-Mib requires the Bridge Mib also be reported. The Bridge Mib is what Intravue uses to determine topology.

Current versions of the Mach switches support the Bridge Mib. If you don't see devices being placed by Intravue under a Mach switch, you probably need to update the firmware of the switch.

Early models of some Hirschmann switches (4000, IP67) reported devices having mac addresses that were numerically close as if they were the same mac. For instance, two devices with mac addresses like 00 00 BC 32 F2 7F and 00 00 BC 32 F2 83 where the last octets are close, could be reported by one of these switches as being on a port when in fact it was not.

These false reports happen infrequently and are only momentary. To work around this problem, Intravue can be configured to require that all switches make some number of IDENTICAL reports

before making a move. In the ...\\intravue\\autoip\\ivserver.properties file: # number of successive consistent switch reports required before allowing device move

# (only increase this if using switches reporting erratic port numbers)

# scanner.switch.move.deferral.count=1

scanner.switch.move.deferral.count=1

Set the count to 2. The difference will be dramatic, but it will take MUCH longer to see real moves.

### **HEWLETT PACKARD PROCURVE 2810**

This switch had an issue responding to SNMP GetNext requests in certain conditions. Software version N.11.15 corrects this behavior.

In Intravue, if the older software is installed in a switch, the switch will not be recognized as a managed switch and it will be placed under an auto-inserted node along with all its directly connected devices

### **HEWLETT PACKARD PROCURVE 1810G**

In early versions of the Firmware the switch added the VLAN-ID to each MAC in its MAC table. The MAC addresses in the Bridge-Mib were incorrect because they contain only 4 bytes of the MAC address, but 2 bytes VLAN-ID. Because of the incorrect MACs Intravue doesn't recognize it as a switch. It is affecting any version of IV. An update to the most recent firmware (V2.x) solves the problem.

### **WEIDMUELLER IE-SW22/2F-M V4.9**

This switch does not report the mac addresses in the bridge mib in numerical order of mac address (OID) as required by the Bridge Mib causing snmp getnext queries to return incorrect data.

### **GARRETCOM**

Early models of GarrettCom switches did not fully support the Bridge Mib. Make sure you are using the latest firmware from their support site.

### RUGGEDCOM

Early models of RuggedCom switches did not fully support the Bridge Mib. Make sure you are using the latest firmware from their support site.

### DELL POWERCONNECT

Some Dell PowerConnect models do not support the Bridge Mib, RFC 1493/4188. They do support the Q-Mib which is a supplement but not replacement for the Bridge Mib. The following models will be recognized as having SNMP by IntraVUE but will not have port numbers and not be recognized as being a managed switch.

- PowerConnect 3448 SW 1.0.0 through 2.00

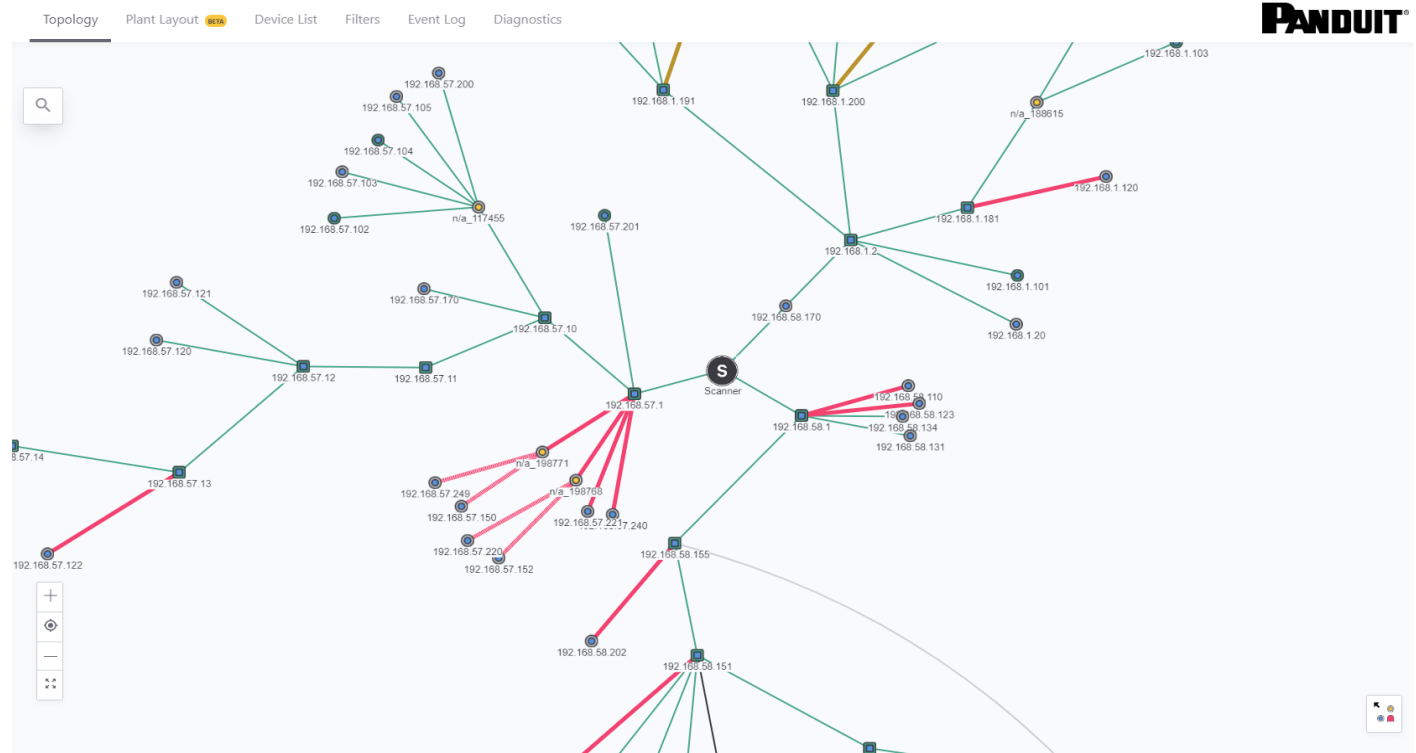
- PowerConnect 3448P SW 2.0.0.21
- PowerConnect 5324 SW 1.0.0.45 Boot 1.0.0.21
- PowerConnect 6224F boot 3.3.3.3

Note that the PowerConnect 3548 SW 2.0.0 does support the Bridge Mib.

### CISCO IE3000, IE4000, C3600 Series, C3800 Series Switches

False Duplicate IP detection on Ethernet modules occurs when using Cisco switches with "IP device tracking" (IPDT) enabled. The modules may go into a duplicate IP address state after a restart/reset. This is a problem with the Cisco switch IOS that is fixed in later models. See [Cisco Switches with IPDT Cause Duplicate IPs](#) for a workaround.

## Topology View



The initial browser view of IntraVUE shows the organization of all devices within each configured network. This is called the **Topology view**.

The IntraVUE™ 3 user interface is provided thru a browser such as Internet Explorer or Mozilla Firefox. On the host computer the URL can always be entered as `http://127.0.0.1:8765`. From any other computer that can ping the host, you may see the same thing by substituting the IP address of the host for the 127.0.0.1, for example `http://192.168.1.55:8765`. Note: the colon and 8765 is required after the IP address and typically you must also enter the `http://` in Internet Explorer.

A [video](#) is available which covers basic navigation, colors, and operation IntraVUE™ 3.

The Top Parent of each network will be one node away from the "scanner" node at the center of the screen. The network is visualized as a star or tree of devices radiating out from the "scanner". This patented method is called a hyperbolic tree.

Individual devices or nodes are shown as colored circles connected by colored lines indicating the connection between the devices.

Drag all nodes on the screen by holding down the left mouse button until the part of the network you are interested in get toward the middle. Attributes of nodes are largest in the middle when you zoom in and they gradually disappear as you zoom out or move in either direction (north, south, east, and west).

You can think of the IntraVUE visual display as a flat network diagram that has been wrapped around a ball, and you can see only part of the ball.

This graphical feature allows very complex networks to be displayed in a single window.

### View Controls

There are several controls that may be used with the IntraVUE user interface.

- **DEVICE** - click on a device brings up a right slider bar with Single View Details including Device Info (Default Details, Advanced Details), Threshold Graph, Events Log.
- **SWITCH** - click on a switch or router brings up a right slider bar with Single View Details (Device Info, Threshold Graph, Events Log), and Sideview Aggregate Details (Multi-Device Threshold Graphs).
- **ROUTER MENU** - click on a device brings up a right slider bar with Single View Details including Device Info (Default Details, Advanced Details, Additional Interfaces), Threshold Graph, Events Log.
- **CONNECTION MENU** - click on a connection line to bring up information about the connecting nodes including Port Information, Ping Response/Failure Graph, and Transmit/Receive Bandwidth Graph.
- **CRTL-KEY LEFT CLICK HOLD MOUSE BUTTON** - to draw an area around multiple nodes to bring up the Threshold graphs just for these highlighted devices.
- **DRAG WITH LEFT CLICK HOLD MOUSE BUTTON** - moves the entire network to shift the devices that are seen in the center or edge of the browser page.
- **ALT-KEY PLUS LEFT MOUSE BUTTON** - shows the line length factor as a black circle. If you continue to hold the mouse button down you may change the size of the line length. This is applied to all lines.
- **HIDE SLIDER** - click on the map view to clear right side slider bar.

- **MULTIPLE DEVICES** - CTRL-KEY LEFT CLICK HOLD MOUSE BUTTON DRAG AREA - opens a slider on the right side showing IP addresses of the highlighted devices.

## Admin Controls

This is another form of the Mouse Controls above. Requires you to login as Admin.

- **SYSTEM MENU** - click on the header bar options (Configure, View, Analyze, Help, About, Login, Topology, Plant Layout, Network List).

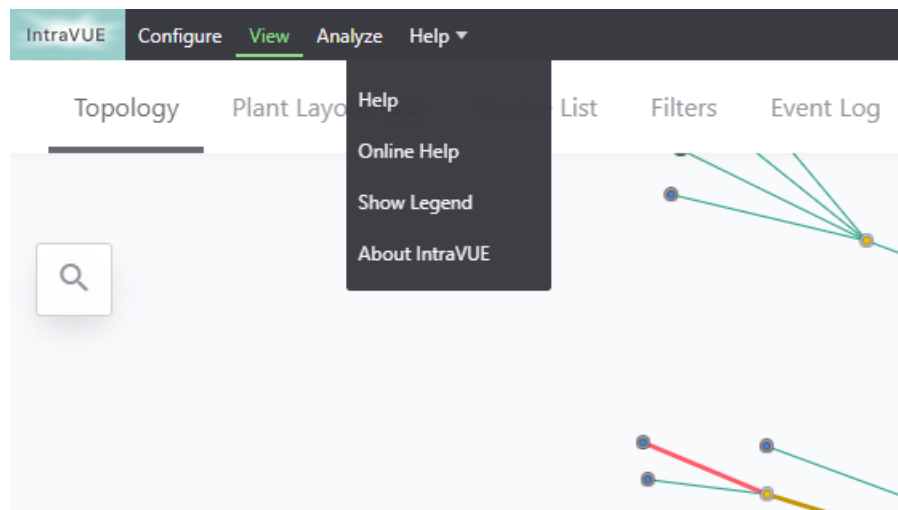
- **DEVICE MENU** - right slider panel with options for device, switch, router, connection,



Network List allows you to display in both Topology and Plant Layout views a subset of configured networks by using the toggle button for each network.

- **EXTRA INTERFACE INFORMATION** - zoom in or zoom out to see the other IPs of devices like routers.

## Help



Under the Help drop-down, there are four options.

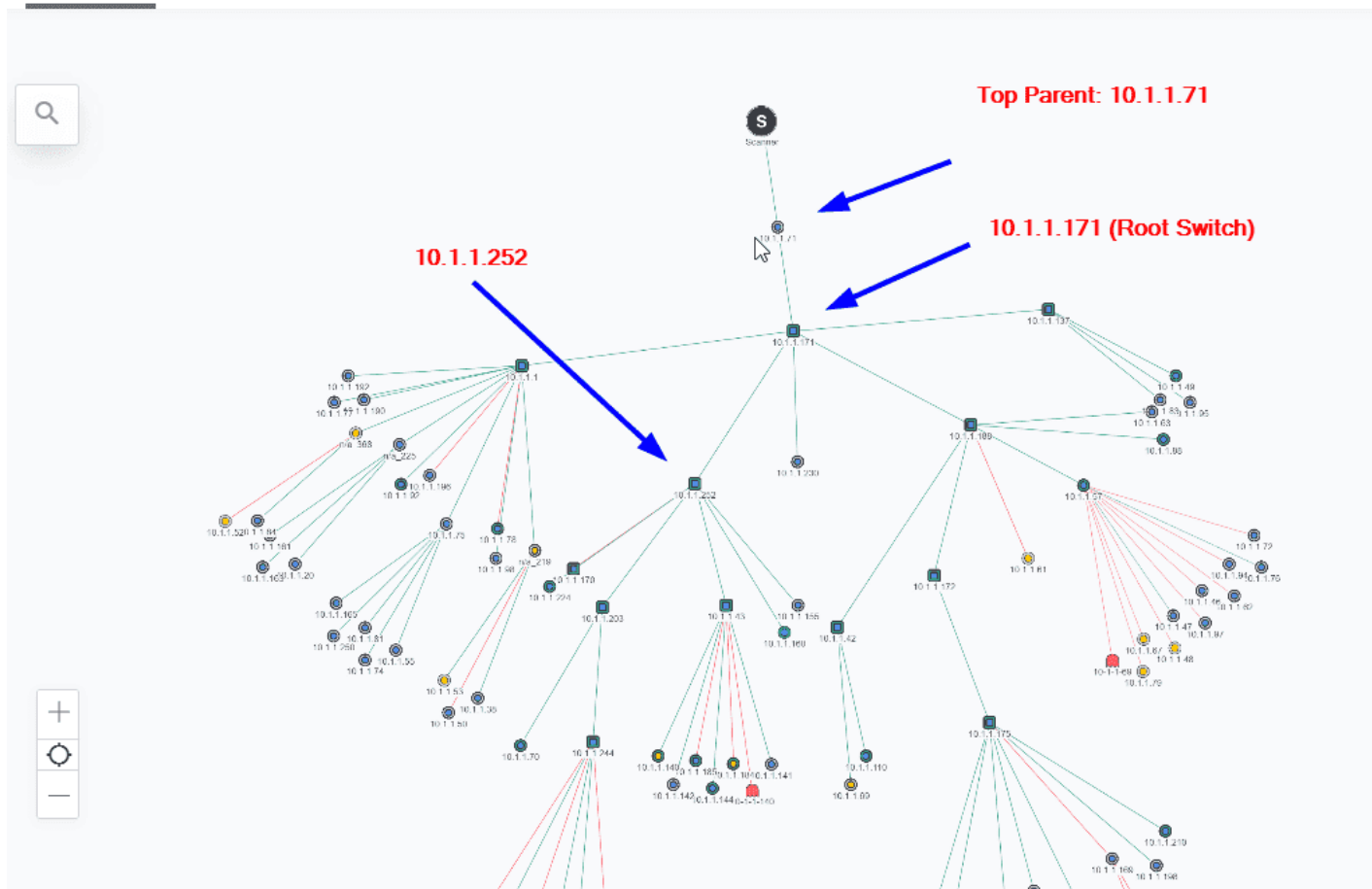
- » **Help/Online Help**- This options brings up the latest version of the IntraVUE Online Help System.
- » **Show Legend** - This enables the node legend at the bottom-right corner of the screen.

- » About IntraVUE - The Version number and expiration date of the IntraVUE service contract can be viewed here.

### Sub-Levels View

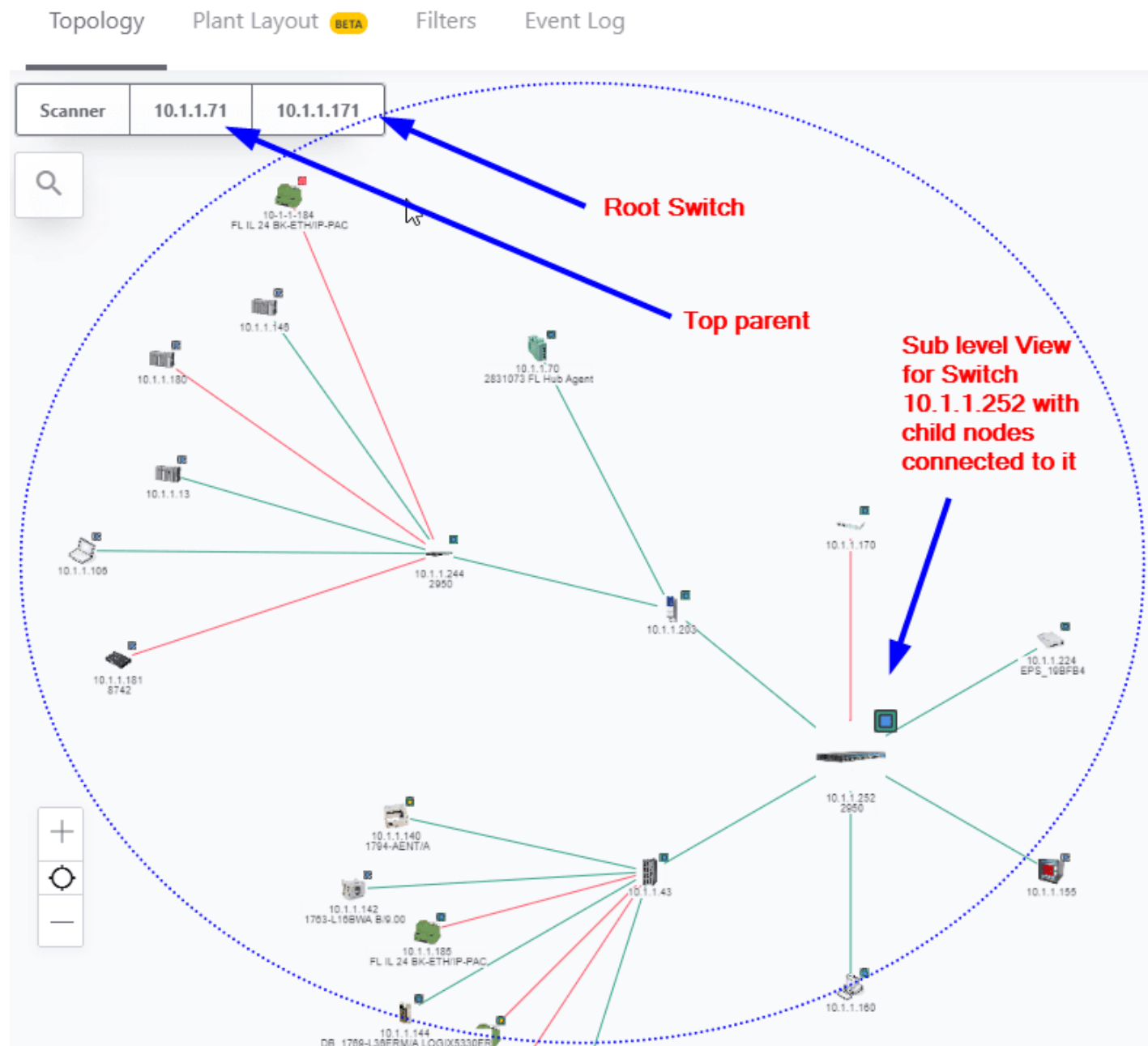


To simplify the view of a complex network, nodes or switches that have child nodes connected to them may be hard to see as the number of nodes in the topology view increases.

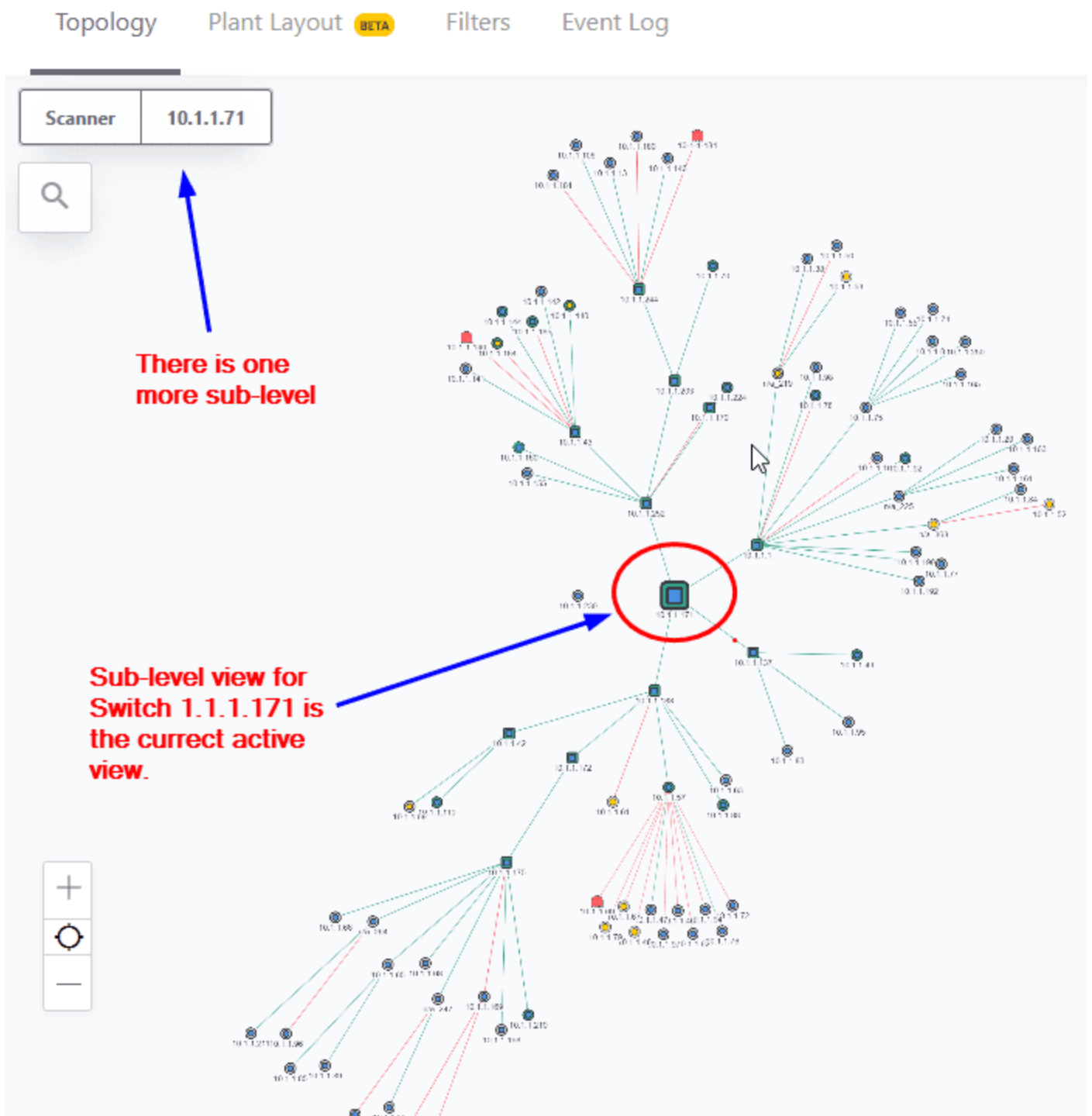
Topology Plant Layout **BETA** Filters Event Log

By double-clicking on a node with many children will reveal all its child nodes connected to that device in the sub-levels view.





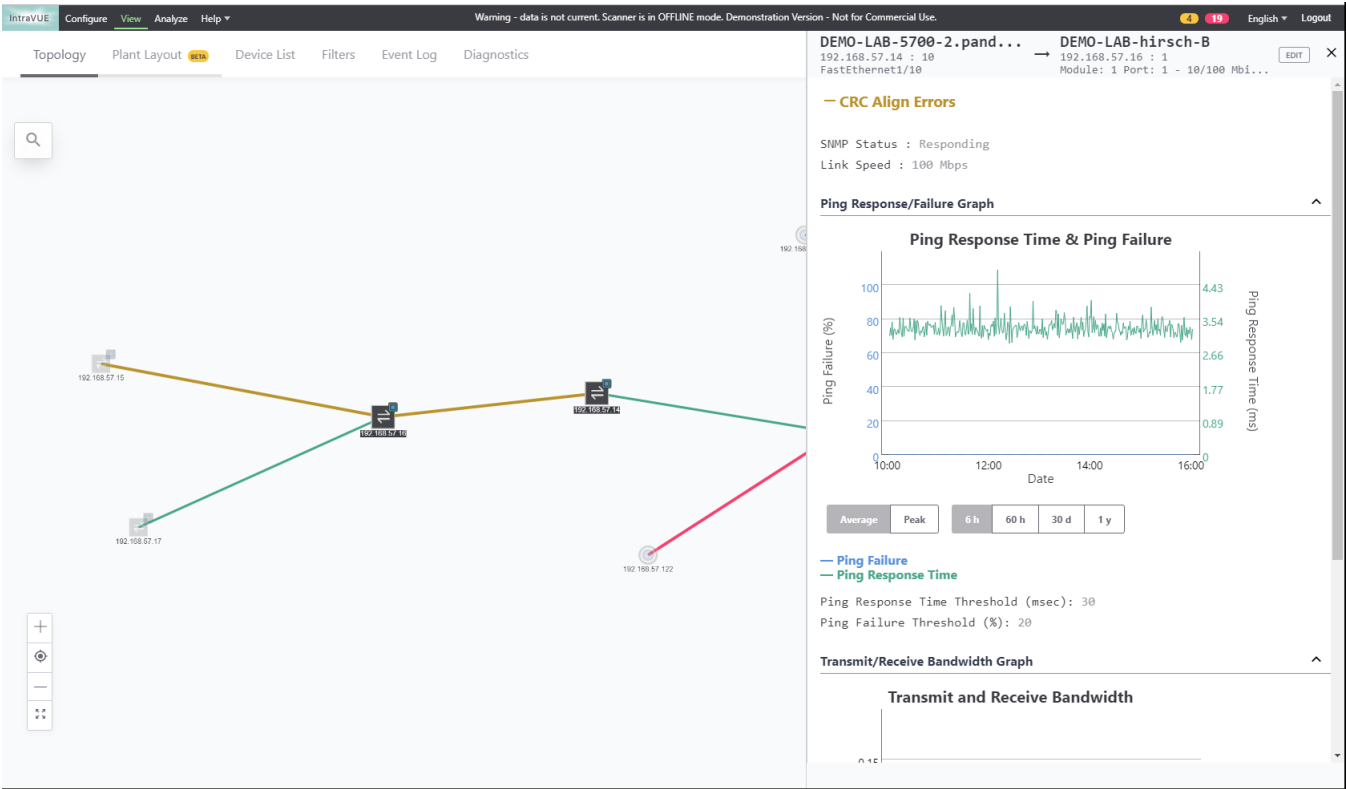
To go up one or more levels in the sub-level views simply click on one of the parent switches IP addresses. If you want to go back to the Scanner Level view simply click "Scanner".



This view does not prevent any alarm or threshold event from occurring.

Alternatively, you can also make IntraVUE™ only show one or a combination of configured IntraVUE™ networks. See [View Filters](#)

CRC in Topology View



Upon clicking connecting lines, this displays a sideview of CRC and IfInError data.

## Glossary

---

### #

---

#### # Devices (KPI By Networks)

Total # of connected nodes that includes devices, switches, and n/a nodes

### A

---

#### Access Control List

(ACL) - A set of rules configured in layer2 and 3 switches that limit what traffic can move from one interface to another or that can be communicate with the switch. ACL's are optional. If enabled, the IP of any device needed to talk to the switch must have a rule that allows that IP. Cisco uses ACL's, other switch vendors have Management Station Lists or similarly named functions that similarly limit who can talk to a switch/router.

#### APT

Advanced Persistent Threat: a group of hackers that develop hacking tools that uses multiple attack vectors for long undetected periods of time in order to compromise and control a target plant network. These tools can by-pass firewalls, IDS, and even Anti-Virus software.

#### ARP

Address Resolution Protocol. ARP is a Layer 3 to Layer 2 protocol used to find to discover MAC addresses associated with IP addresses in a local network.

#### ARP Table

ARP Table (or Address Resolution Table) resolves IP addresses (Layer 3) to MAC Addresses (Layer 2), or Layer 3 Logical Addresses to Layer 2 Physical

## Addresses

### **Auto-IP**

Automatic Private IP Addressing also known as APIPA or Auto IP is a method of automatically assigning IP addresses to networked computers and printers.

### **Avg Device Incidents**

This is the average # of device alerts that have occurred for that IntraVUE network in the last thirty days

### **Avg Switch Incidents**

This is the average # of switches alerts that have occurred for that IntraVUE network in the last thirty days

### **Avg Uptime**

This is the average uptime value in the last thirty days for that IntraVUE network

## **B**

---

### **BootP**

The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951.

### **Bot**

A software application that can be designed for industrial automation environments to operate an automated tasks (scripts) from an infected computer against a single ICS in conjunction with other bots. See botnets, ICS.

### **Botnets**

A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack

(DDoS attack), control devices, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software.

## **Broadcast**

Communications traffic that is sent to all devices in a subnet. A layer 2 switch will typically send broadcast traffic to all ports of the switch. See VLAN which is a technology invented to limit broadcast traffic to certain ports of a layer 2 switch.

## **C**

---

### **CIs**

Critical Infrastructure (e.g. SCADA, TCP/IP)

### **Critical Always On (Critical Status)**

A critical device expected to be on 100% of the time for which uptime and incidents are reported to KPI system

### **Critical Device**

# of devices that have critical status enabled. See definition of a device

### **Critical Intermittent (Critical Status)**

A critical device which may not be connected 100% and uptime should not be reported. All incidents are reported to KPI System

### **Critical Switches**

# of switches that have critical status enabled. See also definition of a switch

### **Cyber Risks**

Cyber risks means any risk of financial loss, disruption, or damage including loss of reputation due to some sort of failure of your ICS. See also Cyber Threats

## Cyber Threats

Threats to control systems can come from numerous sources, including hostile governments, industrial espionage, politically motivated hacktivist groups, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders.

## Cyclic Reduncancy Check (CRC)

he cyclic redundancy check (CRC) is a technique used to detect errors in digital data. CRC is a hash function that detects accidental changes to raw computer data commonly used in digital telecommunications networks and storage devices such as hard disk drives. This technique was invented by W. Wesley Peterson in 1961 and further developed by the CCITT (Comité Consultatif International Telegraphique et Telephonique). Cyclic redundancy checks are quite simple to implement in hardware and can be easily analyzed mathematically. It is one of the better techniques in detecting common transmission errors. It is based on binary division and is also called polynomial code checksum.

## D ---

### Device

A device in IntraVUE can be any node that is not a switch (see switch) and that has either an IP address or an 'n/a' or 'N/A' label

## F ---

### Firewall

A special purpose router with additional rules to prevent traffic from moving between subnets, especially 'inside' versus 'outside' an area

## **Firmware**

is a specific class of computer software that provides the low-level control for the device's specific hardware. Firmware can either provide a standardized operating environment for the device's more complex software (allowing more hardware-independence), or, for less complex devices, act as the device's complete operating system, performing all control, monitoring and data manipulation functions. Typical examples of devices containing firmware are embedded systems, consumer appliances, computers, computer peripherals, and others. Almost all electronic devices beyond the simplest contain some firmware.

## **Frame Check Sequence (FCS)**

The FCS is a mathematical way to ensure that all the frame's bits are correct without having the system examine each bit and compare it to the original. Packets with Alignment Errors also generate FCS Errors.

## **G**

---

### **Gateway**

The router any traffic will be sent to if the destination IP address is not local (in the same subnet) as the sender. If that gateway can not route the traffic, it sends the traffic to its gateway, and so on until it reaches the destination.

## **H**

---

### **HMI**

Human Machine Interface

### **HTTPS**

Hypertext Transfer Protocol Secure. Allows HTTP, FTP, or other unsecured protocols to cross the firewall securely reducing risk due to the potential for traffic sniffing and modification with non-secure protocols.



---

## I

---

### IED

Intelligent Electronic Device is a data conversion device

### Ignore (Critical Status)

A conscious decision was made that this device is not critical. Uptime and Incidents are not reported to the KPI System

### Incidents

Incidents includes all events that cause stop time on planned production for an appreciable length of time (typically minutes or hours). That is, incidents cause availability Loss from unplanned events (e.g. equipment failures). It is calculated like this:  $\text{Availability} = \frac{\text{Run Time}}{\text{Planned Production Time}}$   $\text{Run Time} = \text{Planned Production Time} - \text{Stop Time}$

### Industrial Control System (ICS)

Encompasses several types of control systems and associated instrumentation used for industrial process control. Most common include SCADA, DCS, and PLCs.

### IP Address

The (I)nternet (P)rotocol Address is the logical address of a device within a computer network. It is internally a 32-bit number, typically expresses as 4 sets (octets) of numbers between 0 and 255, separated by periods, like 192.168.100.252. Routers route traffic from one subnet to another based on IP address

### IT

Information Technology. Corporate group that manages the core network but not necessarily the automation networks.

---

## K

---

### KPIs

KPIs are assorted variables that organizations use to assess, analyze and track manufacturing processes. These performance measurements are commonly used to evaluate success in relation to OEE goals and objectives

---

## L

---

### Layer 2 Switch

Traditional switching operates at layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses.

### Layer 3 switch

See Router

### LLDP

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP is formalized in the IEEE 802.1AB standard. LLDP does advertise the hostname, management IP Address, port name and description.

### Local Network

A network where all devices share the same netmask and communicate to each other without leaving the network.

---

## M

---

### **MAC address**

Is a Layer 2 unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used in most IEEE 802 network technologies, including Ethernet\IP and WiFi.

### **MAC Address Table**

A MAC address table (Layer 2 addressing to interface binding), is used on Ethernet switches to determine where to forward traffic on a LAN. aps Mac Addresses to Physical Ports on a Switch

### **Malware**

Short for "malicious software", is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs. It can take the form of executable code, scripts, active content, and other software. Since the beginning of the 21st century Malware is becoming a cyber risk for ICS.

### **Max Device Incidents**

This is the peak # of device alerts that have occurred for that IntraVUE network in the last thirty days

### **Max Switch Incidents**

This is the peak # of switches alerts that have occurred for that IntraVUE network in the last thirty days

### **Max Uptime**

This is the peak uptime value in the last thirty days for that IntraVUE network

### **Min Device Incidents**

This is the lowest # of device alerts that have occurred for that IntraVUE network in the last thirty days

### **Min Switch Incidents**

This is the lowest # of switches alerts that have occurred for that IntraVUE network in the last thirty days

### **Min Uptime**

This is the lowest uptime value in the last thirty days for that IntraVUE network

## **N**

---

### **Network Scanner**

Continuously monitors the configured networks checking for device disconnections, new devices added, and threshold data from SNMP MIB data fields. The scan engine uses Ping and ARP to detect the presence of devices and SNMP to get information about the hierarchy of the network. This information is stored in the database.

## **O**

---

### **OEE**

OEE (Overall Equipment Effectiveness) is the gold standard for measuring manufacturing productivity. It identifies the percentage of manufacturing time that is truly productive. An OEE score of 100% means you are manufacturing only Good Parts, as fast as possible, with no Stop Time. In the language of OEE that means 100% Quality (only Good Parts), 100% Performance (as fast as possible), and 100% Availability (no Stop Time). IntraVUE can help a plant improve its availability and performance increasing its overall OEE score.

## OSI Model

The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

## P

---

### PING

A command used to test if a particular host is reachable using an IP address. Pings use ICMP, 'echo request', protocol. If the sending device does not have a MAC address for the IP address in its ARP Cache, an ARP (broadcast) request will be issued before the ping.

### Product Key

A code that determines which features and options are enabled for a license

### PROFINET

is an industry technical standard for data communication over Industrial Ethernet, designed for collecting data from, and controlling, equipment in industrial systems, with a particular strength in delivering data under tight time constraints (on the order of 1ms or less).

## R

---

### Relational Database (MySQL)

This is the area in which both scanned information, administrator configurations, and events are stored.

## **Remote Network**

A network of devices which must be communicated with through a layer 3 device. The IP and netmask of remote devices will not match a local device.

## **Router**

A router is a networking device (or a Layer 3 Switch) that forwards data packets between computer networks. Routing (and Layer 3 Switches) operate at the transport layer of the OSI model where packets are sent to a specific next-hop IP address, based on destination IP address.

## **RTU**

Remote Terminal Units

## **S**

---

## **SCADA**

A SCADA (Supervisory Control and Data Acquisition) system is used to automate the control of and enable remote monitoring of industrial devices. These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals. A SCADA system gathers information (such as where a leak on a pipeline has occurred), transfers the information back to a central site, then alerts the home station that a leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion.

## **SNMP**

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network

devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

## **SNMP Community**

The equivalent of a password for SNMP communications. It is case sensitive. There are read-only and read-write types. IntraVUE only uses read-only

## **SSL / TLS**

SSL and TLS are cryptographic protocols, both provide a way to encrypt communication channel between two machines over the Internet (e.g. client computer and a server). SSL stands for Secure Sockets Layer and current version is 3.0. TLS stands for Transport Layer Security and the current version is 1.2. TLS is the successor to SSL. The terms SSL and TLS can be used interchangeably, unless you're referring to a specific protocol version. The ordering of protocols is: SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2.

## **STARTTLS**

STARTTLS is a protocol command, that is issued by an email client. It indicates, that the client wants to upgrade existing, insecure connection to a secure connection using SSL/TLS cryptographic protocol. STARTTLS command name is used by SMTP and IMAP protocols, whereas POP3 protocol uses STLS as the command name. Despite having TLS in the name, STARTTLS doesn't mean TLS will be used. Both SSL and TLS are acceptable protocols for securing the communication.

## **Subnet**

A set of Ethernet devices that share a common routing prefix, called a subnet mask. Subnets break a network into smaller parts and are connected at the edges by/through routers. Devices in the same subnet are Local to each other and traffic does not go through a router. To determine what is local to a particular

IP address, the IP address is mathematically combined with the subnet mask to compute a range of IP addresses that is within that subnet. It is VERY IMPORTANT that all devices in a subnet have the same subnet mask and that subnet mask agree with their gateway, meaning that all the IP's have the same first 3 octets or numbers (i.e. 100.32.122.12 and 100.32.122.74)

### Switch

A switch in IntraVUE terminology is commonly known in the industrial world as a fully managed switch with configurable SNMP communities and meets RFC 1493 specification. See also Layer 2 Switch

## T

---

### Top Parent

The device that can provide the mac addresses for IP addresses in a network.

## U

---

### Unknown (Critical Status)

A device which has not been configured for Critical Status and hence not in the KPI System.

### Unresolved Nodes

Devices under the Unresolved node will have all the functionality of other devices in IntraVUE. The Unresolved node serves as a placeholder for devices that can not be properly placed by IntraVUE with some information indicating the difficulty.

### Uptime

The portion of the OEE Metric that represents the percentage of scheduled time that a device is available to operate. Often referred to as Uptime



## User Interface

Applet based. The browser utilizes a hyperbolic visualization methodology that allows a very complex network to be displayed on a single screen. This visualization is integrated into a java Applet that is sent to the Client device. The applet is updated on a periodic basis to allow the most current information to be displayed on any client browser.

## V

---

### Visual Management

Visual management is the process of displaying critical information such as KPIs that relate specifically to production output, efficiency and quality. By displaying this data on the factory floor, employees have a better sense of production levels and tend to strive for higher performance. Visual management also provides actionable information that allows supervisors to better monitor performance and determine, in real-time, areas that may need improvement. The overall result helps to drive productivity throughout the organization by increasing efficiency, quality and uptime.

## VLAN

A (V)irtual LAN is a group of devices configured to communicate as if they were in the same broadcast domain. It allows edge/end devices to be grouped together even if not connected to the same switch. VLANs make it possible to create multiple layer 3 networks on the same layer 2 switch. Broadcast traffic from a VLAN'd port of a layer 2 switch will ONLY go to other ports in the same VLAN, NOT to all ports of the switch as would be done without a VLAN.

---

**W**

---

**Web Server**

Web Server (Apache eTomcat). Provides the framework for IntraVUE servlets and applets.

## Index

---

### A

Active Directory 189

Add Child Device 156

Add IntraVUE Agent 178

Add Network 177

Add Range 178

Adjust Ping Thresholds 189

Admin Verify All Devices 175

Admin Verify Devices - IntraVUE 3 87

Analyze 45

Auto-backup 171

Auto Connect 155

Auto IP 156

Available Scanned Networks 139

### B

Backup Database 173

### C

Clear Database 172

Client

- Access via Client 105

Completing Initial Configuration 65

Configuring SMS Notifications 185

Connect IntraVUE & Key Performance Indicators 77

Connection Side View 133

Conventions 11

Core Features 16

Create Archive 265

Critical Status 149

CSV Column Values 256

## D

Delete Device 157

Delete These Devices 157, 263

Deploying an Agent 341

Deployment Options 27

Device and Switch Incidents 47

Device Configuration 250

Device Configuration - Advanced 155

Device Configuration - Image 153

Device Configure - General 148

Device Configure - Links 166

Device Configure - Other Names 151

Device Configure - SNMP 164

Device disconnected 267

Device Discovery & Management 345

Device Info 132

Device Information 250

Device List View 43

Device reconnected 267

Device Side View 132  
Device Uptime 46  
Devices Not Correctly Positioned 179  
Diagnostic Reports 49  
Diagnostics and Troubleshooting 50  
Diagnostics View 141  
Disable All SNMP Requests 165  
DLR Networks 337

### E

Edit Device Properties 53  
Email Alarm Types 83, 184  
Enable Automatic Historical Backups 171  
Enabling Email Alarms 79  
EtherCat 336  
Ethernet/IP and PROFINET 345  
Event Log 132  
Event Log Descriptions 267  
Event Logging 125  
Export / Import 249

### F

FAQs 378  
Fast or Ultra scanner speed 176  
Fine Tuning 69  
First Login 106

---

## G

Generate Analytics Reports 84

Generate Support Archive 265

Graph 132

## H

How to use the documentation 10

HTTPS 351

## I

Ignore SNMP Bridge Mib data 165

Ignore SNMP Device Name 165

Ignore SNMP Location 165

Importing Device Information other sources 255

Importing Device Names From Third Party Sources 358

Include N/A Nodes 250

Inconsistent Results 75

Installation

    New Installation 95

Installation or Upgrade Instructions 35

IntraVUE Agent 34, 86

IntraVUE Agent - Low Cost Agent 340

IntraVUE Agent Discovery Tool 243

IntraVUE Analytics 42

IntraVUE Appliance Configuration 237

IntraVUE Architecture 92

IntraVUE Benefits 14

IntraVUE Components 93

IntraVUE Diagnostics 269

IntraVUE Legend 117

IntraVUE Logs 228

IntraVUE Placement Options 27

IntraVUE Readiness Checklist 20

IPDT 369

ivserver.properties 216

ivserver.properties File 214

ivserver.xml 217

## K

Keep Current Email Settings 173

Keep IntraVUE Scanner Offline After Database Restore 173

Keeping Track of Port Speeds 318

Known Issues 373

KPI

- Standard KPI
  - 30 Day KPI 46
  - Configure Devices 42, 149
  - Daily KPI 45
- Supervisor KPI 293
  - Installation 296
  - Key Performance Indicators 298
  - Supervisor Configuration 299

## Supervisor Reports

Current KPI View 304

Historical KPI View 308

List View 311

KPI By Network 48

**L**

Limiting VLANs on Cisco Switches 326

Link speed Info 134

LLDP Loop Detection 335

**M**

MAC.override 256

Move Device 157

Multi-Device Configuration Export 55

Multi-Device Graph 258

Multiple Device Side View 263

Multiple SNMP Communities 175

**N**

n/a Nodes 71, 331

NA Nodes 331

NAT 156

Navigation Menu 115

Network Configuration 177

**O**

Overview of IntraVUE 13



### P

Ping Failure 134

Ping Response Time Threshold 134

PKI.critical 256

Placement and Scanning Scenarios 27

Plant Documentation 53

Plant Layout Coordinates 250

Plant Layout View 58

Ports used by IntraVUE 25

Powerlink 336

Predispose.txt File 210

### R

Received Bandwidth 135

Registration or Upgrade 39

Remove Ghost Nodes 189

Reset Plant Layout 177

Restore Database 172

Ring Topology 75

Roaming Devices 144

Rogue Device 87, 195

### S

Scan Speed 176

Scanning

- First scan 66

Scanning Requirements 24

## Scanning Scenarios

Hot Standby Redundant protocol 33

Multiple LANs from a single IntraVUE host using a router 29

Multiple NIC cards and no router 30

Multiple VLANs 32

Networks using VLANs 31

Simple Network 28

Search Devices 123

Selecting the Top Parent 177

Selecting The Top Parent 99

Send Archive 265

Sercos 336

Setting Critical States 42

Side View in Edit Mode 146

Sideview Aggregate Details 136

Single Device Graph 258

SMS Notifications 349

SNMP Read Community 164, 175

SNMP Status 134

SNMP.supress 256

Special Files in IntraVUE 215

Supported Protocols 335

Switch Side View 136

SwitchProbe 205

System Requirements 21

### T

The IntraVUE Agent 85

The IntraVUE folder 211

Threshold Graphs 258

Threshold Settings 132

Thresholds 188

Tools Folder 204

Topology View 107, 416

Transmit Bandwidth 135

trapmailer.xml 217

### U

Understanding Spikes In Networks 321

Unmanaged and Web Managed Switches 201

Unresolved node 70, 95

Unresolved Nodes Problems 101

Updating the IntraVUE Appliance Image 246

Upload Archive 266

URL External 166

URL Name 166

Use SNMP provided MAC for L2 Switch 165

User Defined 1 207

User Defined 2 207

User Defined 3 207

User Defined 4 207

User Defined 5 207

User Defined 6 207

User Defined Fields 207

Using the IntraVUE Appliance as a Server 236

Using the IntraVUE Appliance as an Agent 231

util.jsp 206

Utility Programs 204

## V

Vendor Name from OUI 344

Verifying SNMP on Fully Managed Switches 327

View Databases Offline 350

View Filters 138

Virtual Machines 73, 202

Visio Export 62

VLANs 225

VM Host, Hub, or Non-SNMP Switch 201

VM, HUB, or NON-SNMP SWITCH 156

## W

WAP (all children wireless) 156

Weblinks 250

Windows ARP Bursts 342

Wireless Access Points (WAP) 74

Wireless Devices Preserving Old Data 324